Canadian Nuclear Safety Commission
Commission canadienne de sûreté nucléaire

CMD 18-H4.144

File / dossier: 6.01.07
Date: 2018-04-16
Edocs: 5513041

Oral Presentation

Exposé oral

Submission from Sunil Nijhawan

Mémoire de Sunil Nijhawan

In the Matter of

À l'égard de

Bruce Power Inc. – Bruce A and B Nuclear Generating Station

Bruce Power Inc. - Centrale nucléaire de Bruce A et Bruce B

Request for a ten-year renewal of its Nuclear Power Reactor Operating Licence for the Bruce A and B Nuclear Generating Station

Demande de renouvellement, pour une période de dix ans, de son permis d'exploitation d'un réacteur nucléaire de puissance à la centrale nucléaire de Bruce A et Bruce B

Commission Public Hearing – Part 2

Audience publique de la Commission – Partie 2

May 28-31, 2018

28-31 mai 2018

Canada

Submission to the CNSC Public Hearing on Bruce Power's Application to Renew the Reactor Operating Licence for Bruce A & B

Hearing Number Ref. 2018-H-02

Sunil Nijhawan, Ph.D. P.Eng

SUMMARY

I am a pro-nuclear reactor safety professional engineer who insists on safer nuclear power reactors. The focus of my intervention is on the still abysmal severe accident[1] prevention and mitigation capabilities of the CANDU PHWR nuclear reactors owned by OPG and leased to run privately by Bruce Power under certain licenses by the CNSC. As a professional engineer, my strong objections to a license extension are purely in public interest and based on a number of rational factors that supersede the usual haste and convenience of automatically renewing Bruce Power's license. These also include the obvious obsolescence of the 50 year old reactor design, ageing issues of the long irradiated and embrittled reactor internals and inability to meet today's public expectation of risk. I am also alarmed by the track record of Bruce Power management in ignoring related technical issues they are not forced to address as a condition of renewal. An educated, fact based, convincing case has also not been made by the CNSC staff supporting the license extension. There are justifiable perceptions that a decade old, well greased process of CNSC going through the usual motions to eventually and automatically grant any and all wishes of our nuclear utilities is again in motion. Yet, I am hopeful of reversal in this post-truth era and respectfully summarize in my submission documents, concrete reasons demonstrating why it is in not only the long term interest of Bruce Power equity holders but also in the immediate security interest of this nation that the license renewal be denied. There is a need by the station management to first take immediate and meaningful actions to reduce the resulting risk from severe accidents that have devastated other countries. I submit that there are enough reasonable grounds that the application should be denied for now and any license extension wait until public interest in securing a safer reactor at Bruce is served first. The public safety must never get untethered from the truth.

I am hopeful that the new Commission members will actually read and independently evaluate this submission with all its attachments and not depend upon the talking points that the staff will prepare like in the previous hearings.

[1] *As opposed to the license basis accidents, severe accidents like at Fukushima are initiated by external initiators cascading into multiple safety and process system failures that result in extensive fuel failures with significant core damage or ill-trained station personnel experimenting with the reactor as at Chernobyl.*

RELEVANCE MY BACKGROUND TO INTERVENTION

I am a Canadian nuclear safety professional engineer with about 35 years of safety analyses related service to all segments of the Canadian nuclear industry. Analytical methods that I developed, have contributed significantly to justifying the Bruce station compliance to regulatory safety requirements. My work is documented in Safety Reports in support of Bruce, Darlington and various CANDU-6 reactors for their licensing. I have also developed and continue to develop new and innovative, analytic methods for evaluating progression and consequences of the beyond design basis accidents that contribute most to risk (Level II Probabilistic Risk Assessments). These are large multi-disciplinary analytical models grouped in a number of large computer codes that require special computational algorithms and an understanding of multiple physical phenomena feeding into each other. I have participated in various licensing submissions, design evaluations of advanced reactors and have published regularly; participating in international conferences, focusing for 3 decades on severe accident related issues. I started the integrated reactor response severe accident analyses work in Canada while at Ontario Hydro in late 1980s.

During those golden years of Ontario hydro where I was engaged as a consultant contractor for a decade, we developed a number of new and then innovative computer codes. Some visionary technically savvy leaders (Bill Morrison, Alan Brown, Charles Blahnik) gave me the opportunity to develop indigenous analytical capabilities in the area of unmitigated severe core damage accidents, over a decade before the national regulators or other CANDU utilities worldwide understood its significance or woke up to the need. As understanding in the uncharted territory of horizontal fuel channel reactor damage began to emerge, so did the revelation of design limitations and accident progression pathways we never considered before. We also started developing means of correcting past oversights with hardware improvements that would not affect normal operation but would enhance reactor safety from design basis and severe accidents alike. Not many were implemented as the Darlington reactors were coming on line already.

Over the last 5 years I have been developing the next generation of severe accident related computer codes (ROSHNI series of codes) whose detail and depth dwarf my own work (for example the MAAP-CANDU code) from 25 years ago that I consider now only marginally useful but definitely obsolete and dangerously wrong in places. That code from early 1990s has somehow survived as the gold standard for Canadian and many overseas utilities, while retaining some questionable assumptions, omissions and simplifications. So the consequence assessments that Bruce Power uses in PSAs are of questionable validity and I have told them why. But they love the 'good news' they are able to extract as there are enough screwdrivers in the input to get favourable results that make Darlington and Bruce applications give a lot of comfort to the black box users. Some results like a 5 hour window to restore water to darlington boilers are grossly and dangerously misleading. similarly, the assumptions of a magical core collapse are also wrong.

From the insights of the these new detailed analytical / numerical simulations and from an ability to model complex, inter-related reactor processes, I have gained a substantially different understanding of severe accident progression in CANDU reactors than the one from the 1990s still percolating at Bruce Power. My interventions started when CNSC came out with drums rolling with their so called Fukushima action items to improve the CANDU fleet. From my perspective, all I saw were band aide solutions, plans to make plans and lullabies. I protested the luke warm, defensive response of my industry to Fukushima in Canada and based on my understanding of the technology, offered more robust redesign solutions that can help actually reduce risk.

At Bruce hearings in 2015 I pointed out the inherent CANDU design issues that impact risk and create challenges for successful accident management. I documented my findings and presented to Bruce Power 3 years ago a set of 30 odd concrete suggestions. The then Bruce Power CEO Duncan Hawthorne initially welcomed the suggestions but they were unfortunately all shot down in the usual CANDU industry spirit of being defensive and intolerant of criticism. Meanwhile I have been able to convince overseas PHWRs to think and start acting otherwise. Perhaps they value their people and land more. I have also developed severe fuel damage codes for fuelling machines, spent fuel pools and research reactors and discovered the alarming risk that spent fuel bundles present by the mere geometry of their placement.

I was trained by some of the best in the world and was taught and required to not fear the truth. Needless to say I am thankful for the opportunities granted to me and I have significantly benefitted from them. It is perhaps because of my independence that I am about the lone technical voice from within the industry able and willing to challenge in interest of public good the complacency, intransigence, rot and decline in my industry. My proposals to shed some old design guidelines and improve the risk profile of our reactors, especially in wake of the incomplete, ill-directed and irresponsible response in Canada to the unfortunate Fukushima accident, have to be openly debated.

I seek no glory and have no axe to grind except an overbearing commitment to my country that is being exposed to an un-necessary risk from continued operation, without the necessary design upgrades of a 50 year old reactor technology that is being pushed to exploitation beyond its design life. The industry I have served for over 3 decades now discourages intelligent discourse, promotes propaganda, promotes the incompetent to mamangement, sweeps reactor problems under the rug and pretends that mere band-aids will cure the rot.

While a proud practicing member of the CANDU design and safety assessment fraternity, I have come to a firm conclusion that our CANDU reactors are not perfect and that they were actually not designed by God or her messengers. Having also worked on other reactor types (BWRs, RBMKs, Research reactors) and worked overseas, I am also convinced that we in Canada do not have the exclusive or any bragging rights to overall design excellence. Our own designers, scores of them my good friends, will admit to you and that our reactors are un-necessarily far more complex in places than certain other designs and that not our design decisions were optimized. Case in point is the infamous decision to replace properly designed PHTS pressure relief valves on all CANDU reactors in ~1996 after one at Pickering stuck open. I also believe that we are now adept at hiding certain design flaws and quick at claiming superiority in design of our reactors and robustness of our regulatory regime. I have noticed that over the last 10 years our regulator CNSC has gone into an overdrive in public self aggrandization and self adulation. Certain CNSC staff show subservience to utilities and their response to known problems weighed down by complacency. I have documented[1] and openly discussed the negative impact a compliant, complacent regulator has on safety improvements.

JUSTIFIED FEARS ABOUT LOSS OF CONFIDENCE

With 35 years of working with designers, utilities, regulator both from inside and out, I have seen the safety culture in the Canadian nuclear industry deteriorate significantly and measurably over the last 10 years. We are in a post-truth era now where spin doctors and MBAs have put the scientists and engineers into the trunk behind the back seat. Public safety is essentially only a buzz word now without concrete targets. The utility management is typically non-technical and we constantly import our CEOs from overseas and CNSC members in the past from political ties that served not the public trust but certain 'mandate'. The short term vision of for-profit players who replaced the knowledge based nuclear legacy that thousands at AECL and Ontario hydro built over 3 decades, serves the public interest poorly.

In this post-truth era, regulators have also lost sight of their legislated mission and rubber stamp any and all requests by the powerful private industry that pays its bills. For-hire consulting companies and imported consultants spew out alternative truths on pressing safety issues. Senior CNSC managers depart from truth knowingly in support of the utilities and with impunity. They regularly put out missives bizarrely claiming harmless nature of CANDU severe accidents and the glorious watchdogs for public safety that they are and how they teach the whole world about nuclear safety. They fail to acknowledge any design imperfections that plague the one reactor type they regulate but poorly understand.

It is a situation that pains professional like me as more and more people lose faith in the current regulatory regime and the industry that hides behind it's cost sharing for-hire umbrella. Licensing hearings have become a joke and an inconvenient pit stop towards uninhibited exploitation of a long tired technology in dire needs of a revamp. These are the reasons that this intervention is not an endorsement of the charade that these public 'hearings' are going to be. Yet it is submitted in hope that saner minds may prevail after all here with the new CNSC members or the information so put into record will be useful in a different forum thereafter.

Having specialized in the field of severe accidents, I have professionally investigated the issues for decades and I worry for my people in a manner that may be different than the Bruce Power management does. My sincere advice in the name of public safety is to reject the application pending implementation of real and effective design enhancements and mitigation measures that will allow better accident management and less severe consequences if this obsolete design station must continue to operate at all. *Not mustering the courage to arrive such a decision in interest of public safety and the nation's security, the new Commission would surprise nobody. Like in countless hearings in the preceding decade it would have lived up to the demands and expectations of the industry that largely finances the CNSC operations.* I am encouraged however by the profile of some new Commission members along with my impressions of a returning member who has intelligently continued to raise a few pertinent issues in her questions.

PAST ACCIDENTS REQUIRE PROPER REGULATORY OVERSIGHT

Highly unexpected, unmitigated and very severe accidents have happened in 3 civilian nuclear power reactors in just under 15,000 reactor years of operation in 3 of the most technologically advanced countries within my professional career (TMI -1979 -USA, Chernobyl-1985 -USSR, Fukushima -2011- Japan). As a result, in Canadian public's mind the frequency of severe core damage accidents is orders of magnitude greater (~1 in 5000) than the advertised number of 1 in a million reactor years. The Canadian public can ill afford the price that Ukraine and Japan ended up paying for the incompetence of and disarray within their nuclear establishment s and thus expects more from us in Canada. It expects us to err on the side of safety, invest appropriately in research and development, not bend regulations for convenience and certainly has not granted us permission to take un-necessary chances. It expects a regulator that is not in bed with the utilities it is legislated to oversee. It expects us to not operate obsolete nuclear reactors for profit alone. Similarly, the first responders do not expect to be misled, as they are now, about the environmental effects of a severe reactor accident or timing of the accident progression. The current state of affairs is untenable and the push by the current CNSC management to grant 10 year licenses before someone's retirement is misplaced.

The consequences to the land from the above three reactor accidents have been historically unprecedented to date from any other industrial activity, except war and nuclear weapons. This from an industry engaged in a simple production of mere electricity - a replaceable commodity available from many other sources. The damage they inflicted was not caused by war, alien invaders but by a careless betrayal of trust from within. The effect on the land of these types of unfortunate and largely avoidable nuclear power reactor accidents will last for thousands of years, long after these companies and perhaps even countries cease to exist. Post mortem analyses reveal that these accidents could have been largely avoided by better designed, better fission reactors managed with greater care, humility and competence. Fukushima taught us that timely design upgrades and better training of personnel along with an institutional overhaul are not negotiable issues.

All 400-odd currently operating power reactors in the world can all use retrofits to reduce accident probabilities and reduce severity of their consequences. This has long been realized but has not been practiced in a number of countries including Canada where a blatant collusion between the CNSC management and utility management exists, not unlike the one that prevailed in Japan and the Soviet Union, before the unavoidable consequences punished them for a similar unholy alliance and management arrogance in punishing and trivializing dissent like mine. I am not going away because I know my subject and the technology of severe accident evaluations that I helped establish in Canada. And because I intend now to persevere.

Bruce Power management, with their irreverent attitude to critically necessary reactor upgrades, may one day cause the loss of a ~30 billion dollar plant they do not own and blame the accident initiators outside their control as TEPCO tried to do with tsunami in Japan. Their unwillingness to properly strengthen the reactor defences may also cause additional hundreds of billions of dollars worth of damage to the pristine Bruce Peninsula and the poor unsuspecting US states to the south. It would be borne largely of their arrogant intransigence and a refusal to look at the issues that I bring out as a professional obligation. At this stage only the CNSC members can ignore the obfuscation in the licensee submission and steer the nation away from the likely impending disaster.

My industry has long forgotten the lessons of the worst ever nuclear power reactor accident at Fukushima in mere 7 years. There have been some very bizarre half-truths celebrated as evidence by certain CNSC staff and utility representatives on the consequences of a severe core damage accident in a series of bizarre reports with little technical basis but long winded songs of adulation for the technology they seem to ill understand. The Commission should not forget that it was the collusion between the Japanese regulators and the Japanese nuclear industry that exasperated Fukushima accident consequences. But for the institutional failures, similar to ones we are seeing in Canada now, tsunami was just an initiator that should have been routine to handle for that multi-billion dollar industry lying deservedly in ruins now. Canada can ill afford a similar outcome as the CEO's imported from outside will walk away with us holding the radioactive bag if the reactors are not critically examined and upgraded for their vulnerabilities before we too have an unfortunate initiating event (like the 2003 network event in Ohio) that cascades into a station blackout in the Bruce reactors and turns this beautiful part of the country into a wasteland. There is no mandate anywhere to be that irresponsible and the nation will come back to us in a vengeance previously unimagined by us.

POOR CAPABILITIES FOR A CRITICAL DESIGN BASIS ACCIDENT

What is of great concern is that Bruce Power reactors do not even meet all the old licensing requirements.

For example, postulated accidents such as LOCA+LOECC which are treated in the safety reports within the design basis are now known to be quite poorly analyzed and the mitigating measures that were supposed to keep the accident consequences below regulatory limits are now clearly inadequate. In the Bruce A/B licensing analyses, fuel thermal analyses for LOCA+LOECC are conducted by single channel models that assume a critical, constant critical flow rate of steam into the channel that maximizes oxidation potential of the fuel string. The analyses are typically carried out for a simulation period of an hour during which the 'hydrogen' source term is calculated for a number of representative channels. These source term predictions are based on only fuel channel modeling using computer codes such as CHAN-II or CATHENA. These codes, however, fail to model oxidation by steam and air of other reactor components, especially carbon steel feeders and main heat transport system piping as well as stainless steel end fittings. This omission has safety implications that we propose to highlight and help rectify.

A standalone methodology using detailed material and fluid (D_2O) properties and a discreet end fitting and feeder heatup model was developed an employed to first stylistically illustrate the magnitude of feeder oxidation under the stylized conditions used for (LOCA+LOECC) analyses. It was shown that the actual source term for combustible deuterium may be significantly more than previously considered. Hydrogen mitigation measures, such as igniters and recombiners have been sized according to the predicted source term that is typically of the order of 65 k-moles of H_2 while the actual amount may be 5-8 times higher. As a result, the effectiveness of 'hydrogen' detection and mitigation systems needs to be re-examined and a potential for containment failure due to gas explosions needs to be reconsidered as well. Bruce power likely understands this but has totally ignored this. We are now using a sophisticated integrated analyses using ROSHNI to calculate LOCA+LOECC Deuterium source terms. The issue has been within Bruce Power's knowledge for at least 5 years but they have done nothing to improve the reactor safety systems even for this most limiting of design basis accidents. There are lists of many more safety issues that Bruce Power has ignored or got exemption for from a compliant CNSC staff.

POOR SEVERE ACCIDENT MITIGATION CAPABILITIES - CASE FOR DENIAL OF APPLICATION

While most operating reactors in the world did not include consideration of severe accidents within their designs, most have inherent features that limit off-site consequences with additional built-in barriers like pressure vessels and strong, leak-tight containments that limit off-site releases like at TMI. Bruce reactors have neither. Others have taken the lessons from Fukushima seriously and made extensive hardware improvements in mitigating systems and emergency planning, Bruce Power has barely scratched the surface. Most have made emergency planning for the population at risk consistent with the predictions and history of large releases of radioactivity. Bruce Power has consciously and on purpose, denied possibility of a large fission product releases and considered release of only about 0.1% of core inventory and thus misled the provincial authorities who poorly understand the issues but unfortunately will bear the brunt of it. The accidents at Fukushima saw as much as 30-40% releases of core fission product inventory. Bruce power makes outrageous claims about the effectiveness of the very few EMEs it has installed (like a 10,000 fold retention of fission products in their FCVS). Bruce Power's audacity in presenting severe accidents as being of benign consequence was perhaps emboldened by some bizarre and irresponsible reports put out by the CNSC staff [2,3] . A systemic institutional failure, like one detailed in the Japanese Parliamentary report on Fukushima[4] is brewing in Canada and we are very likely sleep walking towards a similar disaster. Bruce Power management might think that it can play the odds and can afford that outcome. But Canada cannot.

Station blackout (sustained loss for all onsite and off-site AC power leading to a loss of heat sinks) is a standard accident, inherent severe accident mitigation capabilities of all reactors are analyzed for after TMI. Lately the emphasis is on state-of-the-art[5] best effort analyses demonstrating response of reactor systems without operator intervention, without EMEs to investigate if there are inherent defences that limit off-site damage irrespective of the initiating event. Parallel but separate analyses credit operator interventions and effectiveness of engineered emergency measures and severe accident management. This is only the first step in a series of analysis and design evaluations. It is a serious endeavour not limited to desktop exercises, driving out shiny pumper trucks in summer or showing equipment tracking on iPhone apps.

State-of-the-Art Reactor Consequence Analyses (SOARCA) type analysis using computer code ROSHNI, simple design reviews, and parallel studies of a SBO scenario for CANDU reactors have unveiled a number of serious design vulnerabilities that do not exist at other reactors. Some of these vulnerabilities are in the basic CANDU design concept while others are in its implementation. Yet others are in the absence of certain safety systems or in their inadequacy. At Bruce reactors there are many. For example, a loss of heat sinks due to loss of power at Bruce A/B will cause uncontrolled pressure boundary ruptures; premature expulsion of coolant from main loops and from the moderator heat sink; direct and early exposure of core debris and fission product releases to the containment; accelerated production of explosive 'hydrogen' from oxidation of reactor Zircaloy and carbon steel; assured failures with huge fission product releases into the environment from their weakest and leakiest of all reactors in the world containment boundary; with sparsely populated PARS units potentially exposed to high concentration of ' hydrogen' they are unable to adequately mitigate followed by thermo-mechanical failure of the thin shell Calandria vessel not designed to hold molten reactor debris. Actual list is very long and parts are summarized in the NUTHOS paper attached to this submission.

When the opportunity came up to undertake a design review after Fukushima and after the last hearings in 2015, the industry assembled a team directed pointedly to reject all concerns and glorify the little things they had done with shiny pumper trucks and GPS equipment trackers. Fortunately they documented their glaring examples of CNSC and Bruce staff rejection of scientific and engineering facts in a COG report[6] that is at times funny, painful and hurtful but mostly just irresponsible. The work done in support by certain CNSC staff is equally iniquitous.

Given the serious nature of the inadequacies and the questionable track record of the Bruce power management in addressing them in consistency with the trust that goes with the license, their reactors are best retired gracefully now. Should there be a need to continue their operation until replacement power sources are brought on line or more advanced reactors built instead, a number of reasonable design enhancements can still be undertaken. Aim would be demonstrably minimize risk from a severe accident by eliminating or minimizing some of the undesirable system responses that have become so obvious that one questions the wisdom of licensing such a reactor in the first place (just look at the containment design). This has to be an honest industry wide, almost a national priority and not become again an issue of unflinching defence and worship at all costs of the CANDU design. Forget about all the jobs the reactor supports, think of all the lives it will dismantle.

What baffles me most is not just that the Bruce reactors are obsolete and should be retired gracefully before they present a Fukushima sized cleanup bill, but that the management is lethargic and hostile to any criticism of the rather limiting safety features of a 50 year old design when even the ECC was considered a luxury and the reactor was designed to run on primitive computers. They would rather spend a million dollars fighting new information than consider it gracefully and responsibly. I have personally faced that hostility with which any new facts for increased safety are met. The same defensive, parochial attitude that caused Fukushima is pervasive here in Ontario.

Coming back to the analytical methods once again. The currently used integrated severe accident software packages related to CANDU severe accidents within MAAP-CANDU were developed under the constraints of limited understanding and primitive computers of that time.

It suffers from un-necessary simplifications, an unexplained lack of further refinement and intelligent use. The reaction of the Bruce management is that that those tools are 'adequate for purpose' without actually understanding or articulating what the purpose is. In doing so the impact on emergency planning or accident measures is scandalous. Case in point is the choice of numbers, sizes and types of PARS and size and capability of the FCVS. Poorly sized, PARS become flame throwers when actual 'hydrogen' production is 4 fold high and gases explode in FCVS.

The foregoing is some indication of why I strongly oppose granting of a license extension for Bruce reactors anytime before they have been upgraded in a comprehensive manner that reduces the risk from severe accidents to a minimum. The technical basis of my assertions is partly in the attachments to this submission and largely in volumes of analysis and research that I have prepared and will be willing to share with the new Commissioners. The reality is that the 40-50 year old design of Bruce nuclear reactors does not meet the current public need and expectations of risk. All industrial activities, including all means of electricity production entail risk but for nuclear reactors, risk includes certain long term and unacceptable consequences. This risk therefore must be demonstrably, consistently and consciously reduced by all means, especially design enhancements and personnel training.

By instead, opting for smoke and mirrors, my industry seems to expect and demand a natural right to inflict upon my land and people the long term damage that similarly poorly and arrogantly managed reactors at Chernobyl and Fukushima did on theirs. I hope to demonstrate this overwhelmingly in the attachments to my submission, and in my upcoming presentation and any subsequent action.

CRITICAL ISSUES HAVE REMAINED UNRESOLVED FOR YEARS

I summarize below and explain in the attachments, the open issues that have remained or evolved over the last 3 years since the last Bruce power request for a license extension was rubber stamped by the now departed Commission members who survived years of hearings without getting too technical in their queries or too involved in the impact of their decisions on future generations. We all recall how they were duped, in the case of my submission in 2015 into believing by the since departed CEO of Bruce Power (Duncan Hawthorne - a good man) who openly promised to honestly look into proposed design enhancements. What actually followed was a challenge to our naiveté; as the idea of an honest discussion was shot down by the real powers under him and a cover-up was put in motion through the industry mouthpiece COG whose mandate by definition is to preserve status quo.

At a CNSC hearing in April 2015, some CNSC staff had trouble supporting basic science lest it hurt the interests of their masters at Bruce Power (difference between H_2 and D_2 gases for one; steel oxidation for another, ASME rules about pressure relief yet another....) but were happy to coax the CNSC members sleep nod their approval on highly complex issues presented falsely as irrelevant/solved/inconsequential by the CNSC staff at those hearings (one clueless CNSC manager said that during a loss of heat sinks accident, the fuel will get hot but the feeders will not get hot enough to oxidize; another implied that a severe core damage would result in activity release (100 TBq of Cs-137) from equivalent of 4 fuel bundles out of 6000 fuel bundles in the reactor core; a third said without a trace of shame that even this was a million times too conservative).

What has happened in hearings at CNSC over the last 10 years reminds me of the USSR parliament of 1970s where decisions were pre-ordained by the Central Committee and speeches were made and questions were raised in praise alone. We all know how that ended. Only here the charade includes perfunctory, lazy, laudatory questions by CNSC members insulting the intelligence of most observers. The interveners, some exposing inconvenient truths and coming forward at great hidden costs, are not allowed to cross-examine the CNSC staff or the glum utility managers. The hearings have an atmosphere of a love fest with the utility using a nauseating, evangelical language to praise their obsolete reactor's magical capabilities to withstand any accident and cause no harm.

Yet there are solutions within which interests of all can be safeguarded and overall risk minimized. Only if the reactor accident liability was not limited to the real estate price of a mere couple thousand small Ontario houses (uninsurable against nuclear accidents) and if the utility and CNSC managers were required to sleep with families at the reactor boundary....

The issues raised in this intervention need to be addressed and resolved before a final decision on the application is arrived at. The new group of CNSC commissioners cannot decide in favour of granting Bruce Power's request for any license extension without assuring that public interests are met. Commercial interests of the Bruce NGS lessee cannot take precedence, especially in view of their incomplete response to issues raised earlier and their less than honest application. This is important for public good and perception of CNSC integrity. History of CNSC decisions, some most arbitrary but all in the favour of the utilities, over the last ten dark years does not encourage people like me to continue airing these issues. Some see a conspiratorial, vindictive, ruthless, single minded ways in the single minded CNSC quests to grant all industry requests. The hearing system itself is perceived to be doctored as it does not allow any intervener, especially professionals like me to question the CNSC staff who may be misleading the commission members and the public by espousing observations and conclusions with little technical basis. I have a long list of extremely questionable stances taken by certain CNSC staff in favour of the utilities in complete disregard for truth. Some of them are documented in the attached ASME paper on regulatory shenanigans.

With a highly diminished confidence in an honest hearing by the CNSC at the Bruce hearings, I focus on the following severe accident related issues:

1. Bruce reactors were designed in the 70s and are obsolete overall. They do not have an effective containment (at a design pressure leak rate of 2% per hour it is 480 times leakier and at about 0.5 atm design pressure it is 6 times weaker than a typical US PWR containment) and suffer from reactor design flaws that make them un-licensable in any jurisdiction around the world today. The regulations under which they were licensed are poorly implemented (for example, Bruce containment is not leak tested at full design pressure a minimum of once per 6 years as required by R-7[7], section 5.2.2). The present operators are mere leaseholders with no large interest in the mess they will leave behind; hence no interest in spending a dime on safety they are not forced to. Please understand the issues completely and honestly and then force Bruce power to spend the many dimes it will take to make safer the reactors they wish to operate for the next many years.

2. Bruce reactors have not benefitted from the lessons that could have been learnt from Fukushima accident. Investigation of that accident revealed need for relaxing of the regulatory capture and upgrading of the half century old reactor design concept that is the Bruce NGS. Real needs for reactor upgrades have been lost in the hoopla created by the CNSC Action Items that created plans to make plans but resulted in no appreciable increase in understanding of severe accidents, implementation of comprehensive measures to mitigate them or measurable reduction in risk. Any and all industry submissions were accepted and action items dutifully closed without scrutiny.

2. A large number of concrete suggestions based on actual probabilistic and deterministic analysis of severe accidents at Bruce reactors were documented and presented (see attached papers and submissions) but rejected or ignored to a nauseating degree such that even high temperature steam / air oxidation of 10 km of carbon steel feeders was declared implausible; inadequacy and dangers of PARS ignored .....)

3. Regulatory staff joined the utility staff in propagating a terrible lie that the maximum releases after a severe core damage at one reactor unit would be 100 TBq of Cs-137 per reactor unit. This misleads those who must plan for an emergency and hides the fact that the total inventory in the reactor is over 70,000 TBq per unit and the 100 TBq is just a definition of a 'large' release and not actual consequence of a reactor accident in a CANDU unit which has no pressure vessel and spits out the activity directly into the aforementioned leaky containment.

4. Emergency Measures Ontario were misled knowingly by the CNSC and utility staff about the severity of an accident with a result that thousands of first responders required to manage population movements would be put at great risk.

5. No progress was made in improving the safety at spent fuel pools where the bizarre Bruce Power practice of stacking the CANDU spent fuel bundles in fish basket like configurations still continues and the large potential for Zircaloy fires is still being ignored.

6. The technical basis for running Bruce reactor pressure tubes beyond the ~200,000 EFPH is weak and misleading. Consequences of an in-core rupture of a pressure and Calandria tube coincident with a potential loss of Calandria vessel integrity leading to onset of a severe core damage are unacceptable.

A cursory review of some of the design issues I raise was undertaken by COG and CNSC in 2016-2017 after Mr. Hawthorne's intervention. CNSC even brought in some hires from the US which is not exactly the hot bed of CANDU PSA technology. As expected, all issues raised by me were denied as foretold by many. <u>Each and every one of them</u>. This was a concerted effort that included some obscure consultants imported from the US; people who will have trouble spelling out the acronym CANDU but who were happy to say for a few dollars that they were 'experts' and that they saw no merit in my technical submissions; for example differences between D_2 and H_2 which would make the current combustible gas controls inaccurate and insufficient. Their denial of basic science and the denial of an opportunity for me to cross examine them and examine their evidence brings me back to this forum. The CNSC commission was represented by a lone commissioner (one Mr. McEwan?) who berated me publically as an 'outlier' and told me that his 'research' could not unearth and information in support of my concerns about difference between two gases D_2 and H_2 (the industry preparing to detect, measure and mitigate H2 while the reactor accidents will produce an entirely different gas D_2). Imagine if he was to tackle something a bit more complex. I cannot wait to discuss these matters in a more competent and fair forum that has public health and safety at heart rather than other self interests or is bogged down by incompetence.

ATTACHMENTS ARE PART OF SUBMISSION

In support of my submission and for your education of Bruce CANDU reactor severe accident vulnerabilities, I attach the following three documents with the fourth to be submitted shortly:

1. My intervention opposing the Bruce relicensing in 2015. Nothing has changed since that time and I stand behind that submission.

2. An internationally adjudicated technical paper on design flaws and severe accident related vulnerabilities in CANDU multi unit reactor stations such as those at Bruce NGS entitled " *Conversations about Challenges in Multi-Unit CANDU Reactor Severe Accident Mitigation Strategies, Paper N11P0543, NUTHOS-11: The 11th International Topical Meeting on Nuclear Reactor Thermal Hydraulics, Operation and Safety, Gyeongju, Korea, October 9-13, 2016.* ". It includes additional issues.

3. An internationally adjudicated technical paper entitled " *Regulatory Actions That Hinder Development Of Effective Risk Reduction Measures By The Nuclear Industry For Enhanced Severe Accident Prevention And Mitigation Measures After FUKUSHIMA, Proceedings of the 2016 24th International Conference on Nuclear Engineering ICONE24, June 26-30, 2016, Charlotte, North Carolina* ". It details my concerns about advertised CNSC competence and impartiality.

4. My review of the technical basis of extending the pressure tube fitness for service to about 300,000 EFPH which is about 50% more than the original design of components that have seen multiple failures and billions in expensive replacements (report to come later).

I also urge the Commission to investigate all agreements between the CNSC staff and the utility that contravene, relax or ignore any sections of the AECB/CNSC regulations and engineering codes and standards under which they were originally licensed. Case in point is the pressure testing methods and frequency for the containment structures.

I remain committed to supporting safer nuclear reactors and as a professional engineer I feel compelled to raise the issues that I believe make the Bruce reactors currently unfit for exploitation beyond the commitments already made.

Sunil Nijhawan, Ph.d, P.Eng.
98 Burbank Drive,
Toronto, On M2K 1N4
416-414-6499

REFERENCES

[1] 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

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

[3]www.nuclearsafety.gc.ca/eng/resources/research/technicalpapers-and-articles/2015/2015-severe-accident-progressionwithout-operator-action.cfm

[4] The National Diet of Japan, The official report of The Fukushima Nuclear Accident Independent Investigation Commission, Executive Summary, Kiyoshi Kurokawa chairman, 2012

.

[5] State-of-the-Art Reactor Consequence Analyses (SOARCA) Report (NUREG-1935), 2012

[6] JP-4534_Final Report_R0-6 Oct, Final Report on CANDU Post-Fukushima Questions, Prepared by Aj muzumdart, COG Project Manager, Reviewed by Joan Higgs, Bruce Power, Oct. 2016

[7] R-7, AECB Regulatory Policy statement, Requirements for Containment Systems for CANDU Nuclear Power Plants, 1991

ATTACHMENT 1

Revised Submission to the CNSC Public Hearing on Bruce Power's Application to Renew the Reactor Operating Licence for Bruce A & B

Hearing Number Ref. 2015-H-02

Sunil Nijhawan, **Ph.D. P.Eng**

SUMMARY

The premise of this intervention is to put on public record a request for CNSC commissioners to require Bruce Power to demonstrate that the Bruce CANDU reactors have been comprehensively analyzed for their transient response to events that lead to severe core damage accidents and that accident progression, source terms for flammable gases, fission products, energetic interactions as well as off-site health and economic consequences have been analyzed considering all hazards and full detail, using state of the art technology (Figure 1). Bruce Power must also demonstrate that appropriate mitigation measures have already been taken to ensure maximum risk reduction and that all possible avenues of risk reduction have been examined in interest of public safety. This document includes a detailed list of relevant questions that must be raised, issues that must be dispositioned and measures that must be taken prior to any licence renewal.

The other aim of the intervention is to bring to the attention of the stakeholders that the economic risk greatly outweighs the effort required to reduce the vulnerabilities to enhanced risk from severe accidents that are being ignored. For example, the Bruce Power shareholders may not be aware that decisions have been made by a flawed regulatory decision to recommend that Bruce Power take a billion dollar gamble on a fuel channel or a boiler rupturing on a loss of power (long before any core damage for an event terminable without damage) and not replace two $38k safety relief valves that are not only 'bad actors' according to Bruce Power's own OpEx but currently fail to provide over pressure protection so adequately and routinely provided at all power plants and required by law and engineering common sense. The residents close to Bruce A/B reactors may not be aware that the same decision can potentially cause extensive damage to their environment in case of a simple sustained station blackout, long before any of them are evacuated.

The intervention also aims to encourage the Canadian regulator CNSC to take a more neutral and informed role in the field of severe accidents. There are a number of examples in the intervention that clarify for all concerned the enormous risk involved in CNSC assuming the role of a proponent by, for example, publishing unrealistic reports on consequences of severe accidents, a task neither within their mandate nor technical competence. While expedient and convenient in the short term this can result in fateful avoidance of risk reduction for both public and Bruce Power shareholders. Have we learnt nothing from Fukushima, many should ask.

RECOGNITION OF OPERATIONAL SAFETY OF BRUCE REACTORS

We all commend Bruce Power operations personnel for maintaining an enviable safety record for their CANDU reactors during normal operations. The recent operational record testifies to continued excellence and professionalism of the current contingent of the power workers; inherent strengths in CANDU design and to the technical acumen and hard work of the thousands of personnel who are or have been involved in the past in Bruce A/B units' design, construction, commissioning, maintenance, operation, management, support and upgrades over at least 2 generations. Many of them have been my colleagues for the past 30 years and I know that they share with me a commitment to keeping the reactors not only economically viable but also safe, functioning as responsible, reliable contributors in the electricity grid. They will tell you that with great care, the Bruce CANDU reactors will operationally perform as designed and the task of keeping them within norms is not trivial.

LESSONS FROM FUKUSHIMA MULTI-UNIT SEVERE ACCIDENTS

It has been 4 years since the Fukushima accident destroyed 4 reactor units; adversely affected a couple hundred thousand lives and caused equivalent of many tens of billions of dollars in damage. Of many investigations that followed, the one by the National Diet *(parliament)* of Japan Nuclear Accident Independent Investigation Commission (reference 1) stands out in its conclusions:

> *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.*

Another review (reference 2) summarized the root causes of Fukushima as:

- Institutional and regulatory failure
- Inappropriate safety culture; over confidence on NPP safety
- Insufficient expertise with decision makers
- Insufficient understanding of severe accident phenomenology & progression
- Improper accident management
- Improper and insufficient understanding of reactor conditions
- No timely advice sought or available from external experts
- Insufficient exchange/transfer of information among and within organizations

This report recommended :

- Strengthening of safety culture, including an independent assessment system
- Practical countermeasures against severe accidents
- Improvement of NPP procedures, covering up to extreme severe accident scenarios
- Enhancement of NPP instrumentation
- Improvements in diversity & reliability of emergency power supply systems
- Reliable decay heat removal by strengthening passive safety
- Improvement and strengthening of defense in depth strategy
- Effective nuclear safety research and sharing of research outputs
- Enhancement of regulatory standards
- Strengthened independence & expertise of regulatory organizations
- Emphasized role and enhanced capability of operating organizations

Given what we know now about consequences of severe accidents in general (worldwide there have been 3 severe accidents in about 15000 reactor years of nuclear power reactor operation) , I do not believe that there is any justification for continued unfettered operation of Bruce reactors (or of any other CANDU reactor on Canadian soil) unless significant upgrades are made immediately in a number of critical areas related to developing further understanding of accident progression and demonstrable risk reduction from severe accidents.

Unless the Commission members and the Bruce Power management totally absolve themselves of the responsibility vested in them, necessary upgrades to Bruce reactors and a serious re-evaluation of accident progression leading to simulator development and direct operator training in severe accident issues should be a condition to their continued operation under a new licence renewal. Any units that are refurbished should meet advanced risk reduction requirements, design requirements and risk targets significantly more detailed than those currently let loose.

PUBLIC EXPECTATIONS OF RISK REDUCTION FROM THE UTILITIES

While it is recognized that Bruce nuclear power plants were not designed with severe accidents within their design basis, the public perception of risk has changed since Fukushima and an outcome akin Fukushima to a sustained loss of power, however caused, is not an acceptable outcome. No industrial activity should be allowed to have a risk attribute that significant. Thus a decision should be made to quantify the risk and undertake concrete actions to reduce it as soon as possible. The CNSC Action Items (reference 3) were a good start in that direction but have been incomplete in scope, ineffectively planned and poorly implemented. The haste with which a number of Fukushima Action Items were declared 'closed' by CNSC staff in 2013 reminds one of the tacit agreement between the Japanese regulator NISA and the utility TEPCO that Fukushima investigation report for the Japanese parliament blames the lack of Fukushima station preparedness on. The onus in Canada should be on the licensees to demonstrate to the public that risk reduction measures are in place and not just planned on paper. Long term license extensions should be based on completion of risk reduction, not on promises of making plans to do so.

If Bruce Power is unable to demonstrate in good faith that they have acted expeditiously and without reservations in this matter, a licence extension should be made contingent upon their addressing severe accident related weaknesses in design and preparedness within a specified, but short period of time (~6 months). It would be insufficient to write that plans have been made to make plans to do the CNSC prescribed items as stipulated by the CNSC Action Items (reference 3). Bruce Power must demonstrate that they independently have quantified the risk and taken concrete measures consistent with the safety culture[1] expected of them. The attached list of technical questions (page 23) is a good starting point and I will be happy to provide further technical assistance on each of them. Anything less is an abrogation of trust and duty by both CNSC members and the utility.

Those who understand principles of reactor safety and licensing will also tell you that these reactors, like most reactors of that vintage worldwide, were not designed with severe accidents within their design basis. Many of us who have worked on severe accident issues know now that the Bruce CANDU reactors, as they were prior to Fukushima accident in March 2011, will fare rather poorly in the low probability event of a station blackout initiated severe core damage accident similar to that befell 4 reactor units at Fukushima just 4 years ago. We know also that off-site consequences at Bruce A/B reactors of a sustained and unmitigated loss of power event, however caused, will be at least as bad as, if not many times worse than Fukushima for a number of reasons. The list is dominated by extremely high potential for large amounts of hydrogen production, weak containment with layout that promotes high local concentrations of hydrogen and poor mixing. Therefore the issue of the high risk (low probability multiplied by very high consequences) from severe accidents is important not only for the utility but also the regulator acting in interest of public safety.

[1] "Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance." - International Nuclear Safety Advisory Group of the International Atomic Energy Agency (IAEA) (1991), Safety Culture (p. 4)

In my discussion below, I will give details of two examples where CNSC has dropped the ball and is treating the severe accident mitigation issue as a paper exercise, rather than as a serious issue requiring multi-faceted response. I also give a number of examples of how there has been practically no evaluation of severe accident related risk from continued operation of Bruce A/B reactors and include a large number of pointers on what needs to be included in the risk evaluation. I will also affirm that risk reduction needs to be undertaken prior to any licence extension and provide a number of engineering solutions that can be implemented to reduce risk.

It is hoped that CNSC and the utility will finally review their commitment to public safety and undertake concrete actions rather than the smoke and mirror, show and tell attitude of hoping that no technical challenge to their decision of doing as little as possible, is forthcoming.

Whether the two entities (Bruce Power & CNSC) can recognize previously un-availed opportunities in increasing station safety from ideas raised by this and all interventions will decide whether public interest is safeguarded or Bruce Power is again rubber stamped a licence extension without conditions related to necessary severe accident related upgrades to design, operations, safety assessments, emergency planning and off-site support for risk reduction.

SAFETY CONCERNS FOR SEVERE ACCIDENTS IN BRUCE CANDU REACTORS

With a background of actively working in the field of CANDU severe accidents for 25 years, I will try again in this submission, just as I have tried in previous submissions, to describe why the CANDU reactors, that we are so proud of as the apex of multitude of remarkable Canadian innovations, require design and institutional changes now to meet the challenges posed by their inherent vulnerabilities to accidents that fall a bit within (LOCA+LOECC[2]) but mostly beyond (severe accidents) their original design envelope. This time, however, I also look forward to the opportunity provided by these hearings to engage the stakeholders in direct technical discussions of my concerns.

So why are the CANDU reactors so good and profitable in normal operation, so different in their response to a severe core damage accident and why risk from them is so great that guardians of public interest must put conditions on their continued licensed operations? Here is a summary. (Details are in a sequence of events list later).

Simply put - for a simple case of unmitigated loss of all electric power as in Fukushima, our CANDU reactors have no PWR like pressure vessels to isolate the core debris and would thus immediately discharge un attenuated radioactivity directly into 'containment' as soon as a core damage starts; reactor process systems including the PHTS, moderator, shield tank have inadequate over-pressure protection for severe accident thermal loads and thus vulnerable to uncontrolled ruptures and containment bypass; the multi unit plants such as Bruce A/B have no effective power reactor containment like structures around the reactors and rely on a single vacuum building, far too small to service a single unit severe accident let alone a multi unit accident; and the reactor cores have far too much Zircaloy (~ 60000 kg) in fuel channels and too much carbon steel (> 10 km of feeders with over 2000 m^2 of surface area) in feeders that would produce flammable deuterium in amounts (see Figure 6 for relative oxidation potential of carbon steel and Zircaloy and be surprised) that would be unavoidably explosive in short order and cause reactor building breeches exposing the unsuspecting population to radioactivity long before any evacuation can be affected. Inevitability of early failure of containments[3] and of reactor structures and release of huge amounts of activity outside the reactor boundary is easy to demonstrate. We have known this for over a decade and have raised the concerns about enhanced severe accident related vulnerabilities that may cause an earlier containment breech/failure internally and in technical forums. The expectation was that appropriate measures would be implemented to reduce the vulnerabilities. What we saw instead was a lot of talk (e.g. Fukushima Action Items) but no concerted efforts. Almost all Action Items involved multi year paper plans to make work plans. A number of Action Items like Passive Auto-catalytic recombiners (PARS) were tick marked 'closed' irresponsibly in 2013 even while the industry had not done anything to deserve the accolades. Interventions by public were irresponsibly brushed aside.

[2] Loss of Coolant accident with a Loss of Emergency Core Coolant Injection – a low probability accident analyzed in Bruce safety reports within the design basis but without necessary consideration of the large source of Deuterium gas (heavier isotope of hydrogen) that is highly flammable similar to the lighter Hydrogen that wrecked Fukushima.

[3] Multi unit CANDU plants do not have classical nuclear power reactor containments; the reactor buildings and the vacuum buildings cannot pressurize like classical power reactor containments can.

Many of my colleagues who have given their professional life to the CANDU industry will cringe at the knowledge of the current holders of the baton ignoring for over a decade, the warnings about the vulnerability of the designs with inadequate over pressure protection and propensity to produce copious amounts of flammable Deuterium gas and unfathomable off-site consequences. As men and women of professional integrity, they would want to shield the public from un-necessary risk and not produce 'good news' reports like the March 2015 CNSC fiction – "An Update on the Study of Consequences of a Hypothetical Severe Nuclear Accident and Effectiveness of Mitigation Measures" that has no relevance to ANY severe accident in ANY Candu reactor as the source term it uses is just a number picked out from thin air[4]. If that is the extent of technical competence at CNSC in looking at severe accidents and their consequences, the Commission members need to be alarmed. Public needs to be forewarned. New methods of technical discourse developed. Requests to deny licence extensions made.

Canada is perhaps the only jurisdiction where the regulator is totally ineffective, yet loudest in its pronouncements of being a 'watchdog' (a word many detest along with 'lapdog') and the industry brazenly does as little as they can get away with (case in point is their support for the new CNSC 'study' on severe accident consequences – I will summarize the audacious industry input at my presentation and in a supplementary publication).

Those who understand CANDU design, risk sensitivities and the list of vulnerabilities and design fixes I have compiled, agree that a structured approach to fixing the design and implementing effective preventative and mitigating measures, along with serious attempts at training the operators is within our capabilities. In Canada we have adequate technical resources to meet the challenge, only if the upper management at the regulatory bodies and the utilities can provide the necessary leadership or get out of the way of the technical personnel. Bruce Power shareholders are ill served by management collusion with regulator and should require the management to work instead in their long term interest that is best served by making the reactors safer, not just cheaper to operate.

We cannot pretend anymore that severe accidents occur only in other jurisdictions or that our reactors are somehow superior. PHWR is a different technology but it is dangerously delusional to think that CANDUs represent a superior technology as far as severe accidents are concerned. We can only make a collective decision to accept any level of risk but the risk must be properly quantified. This has not been done for Bruce reactors. The PSA numbers presented in the Bruce Power submission mean nothing as the a comprehensive evaluation of accident progression and consequences is still incomplete. A number of commonly accepted targets on releases (< 100 TBq of Cs-137), containment failure (none for 24 hours) cannot be met and so not discussed by Bruce Power. We can not accept the risk from continued operation of Bruce A/B reactors without its quantification by Bruce Power and verification by independent experts.

[4] The CNSC author's response to picking a target release rather than a predicted release is " *Detailed aspects of severe accident progression and CANDU designs were not part of the scope of the study. A generic large release at the safety goal limit was assumed, reflective of the radionuclide mix in the Darlington reactor units. As a sensitivity analysis, the source term was increased by a factor of 4 to represent a multi-unit accident (e.g., 4 units at Darlington)*." This is not a justification for an irresponsible act of denying the public the emergency preparedness measures it deserves and expects from CNSC staff hired to provide the necessary protection. Release from 4 units into a common containment can be 100 times higher, maybe 1000 times higher or just 2 times higher – but the factor must be determined analytically and with reason. Shutting down the plants until this can be done properly would be a more honorable option. Picking a number out of thin air is irresponsible.

We can brace the populace for consequences or we can work together to reduce the risk.

As a nuclear safety engineer who first in Canada started a systematic integrated evaluation of severe accidents in CANDU reactors in 1988 when some very technically progressive and visionary leaders (Dr. Alan Brown who headed Nuclear Safety Department and his legendary boss Bill Morrison) at erstwhile Ontario Hydro decided, without any prompting by and in spite of open skepticism by the regulators (any evaluations would be speculative – one CNSC Director wrote in his great wisdom), to start evaluating progression of and consequences of severe core damage accidents. I was engaged to analytically integrate the understanding of DNGS reactors under degraded cooling conditions and develop an integrated computer code that modelled response of all major systems to severe accident phenomena in one package. After 5 years of effort I developed a code, which did such evaluations albeit with multiple limitations, and that code – MAAP-CANDU is still used by the industry. The code contains about 50% of material, mostly irrelevant for CANDU accident progression evaluations, from an EPRI code for LWRs called MAAP. I last worked on that code in 1993 but have continued to work on severe accident issues uninterrupted to the date. After years of frustrating wait to see further innovations and development in the MAAP-CANDU methodology to better predict accident progression and consequences, I have a new, significantly advanced severe accident code ROSHNI that I now use to calculate CANDU severe accident progression and consequences. In addition to having the support of actual calculations, my observations are based on the 25 years of severe accident progression and design evaluation experience so acquired.

After over 25 years of working on the topic of severe accidents, I understand now that the CANDU reactors, especially the multi unit plants such as at Bruce need serious upgrades to reduce risk from severe accidents and that our understanding for DNGS units in 1993 was primitive and the MAAP-CANDU (now under a new name MAAP5-CANDU although there were no MAAP1-CANDU, MAAP2-CANDU or MAAP3-CANDU) computer code is incomplete and devoid of any serious improvements in CANDU related modelling in the 22 years since its first release.

I have openly shared that knowledge with the industry and seen the circus around the Fukushima Action Items at CNSC degenerate into a farcical charade culminating in CNSC publishing and as of March 10th 2015 republishing without much change, a study on consequences of a severe accident at CANDU reactors with an impossibly small source term (100 TBq of Cs-137 out of a total of ~70-100,000 TBq in one unit) totally devoid of any supporting analysis on how an accident would actually progress in a CANDU reactor (authors at CNSC perhaps did not know how that was to be done). How come not one commission member ever clued into the study having no merit, being of dubious quality and dangerous for emergency planning purposes given that the source term was fictitious and represented a wishful target? Although I must say that a couple of Commissioners continue to ask some of the right questions and give me hope.

SEVER ACCIDENT PROGRESSION PATHWAYS THAT IDENTIFY DESIGN VULNERABILITIES AND RISK

I will summarize some of the issues by using an easy to understand Station Blackout (SBO) scenario. Just because we cannot have an ocean tsunami at Bruce reactors does not mean that a sustained loss of AC power event cannot be caused to happen and consequences cannot exceed those at Fukushima, an accident initiated by nature but considered totally avoidable and blamed on human errors including regulatory incompetence and industry arrogance for its consequences (reference 1). All jurisdictions with responsible regulatory regimes require that progression of accident and consequences of such an event be evaluated to demonstrate effectiveness of existing systems and containment structures for at least 24 hours. Far too much emphasis has been placed on Level 1 PSA in Canadian risk assessments and the actual processes required to evaluate accident progression (research, code development, analyses) have been neglected in deference to speculative hyperbole about CANDU superiority.

Here is a summary of overall progression of the station blackout accident in a CANDU reactor at Bruce[5]:

> *After all AC power is lost, the reactor trips and reactor thermal power drops to about 5% in 5 seconds, 2% in about 20 minutes and 1.5% in about 1 hour.*
>
> *Feedwater injection into the 8 Bruce boilers drops and then stops a few minutes after loss of power. Heat transport system that circulated heavy water around the fuel channels depressurizes to just above the secondary side pressure but continues to circulate coolant through the boilers due to density difference induced flows (thermo-syphoning). Fuel remains adequately cooled at decay power levels. Boilers (also called steam generators) remain an effective heat sink as long as they have sufficient inventory of light water.*
>
> *As soon as the depleting boiler secondary sideinventory falls too low to remove heat from the thermo-syphoning water flowing in fuel channels (~1-2 hours) the heat transport system re-pressurizes. Recall that no operator action is credited in this scenario and no addition of water into boilers from feedwater train considered.*
>
> *At this time the first unintentional error in CANDU design becomes critical. The system re pressurizes and attempts at this time to avoid an over pressure by rejecting the decay heat through safety relief valves but an inadequate steam relief capacity (tests for Bruce safety relief valves confirm this) leads to a continued over pressurization. These pressure relief valves were reportedly properly designed in the original Bruce units but erroneously mis-sized in 1996 after a knee jerk reaction (and poor engineering decision) to a 1995 event at Pickering.*

[5] A station Blackout scenario includes loss of all AC power, including emergency equipment. No cause necessarily specified. No operator actions credited. The sequence of events is almost identical for single unit plants as well except that they do not sport a vacuum building but have a half decent containment, absent in multi unit plants at Pickering, Darlington and Bruce stations. There is only one operating single unit plant in Canada – at Pt. Lepreau in New Brunswick. The other at Gentilly in Quebec was shutdown for decommissioning by Hydro Quebec in 2013. There are others in Korea (4), Argentina (1), China (2), Rumania (2), Pakistan 1) and India (12 – only 1 of Canadian origin in operation).

So, a boiler dryout leads to an unusual for a nuclear power reactor, over-pressurization of the Heat Transport System and an unavoidable, uncontrolled failure of a pressure boundary component. The failure is most likely to be in ever so vulnerable boiler tubes, resulting in a potential containment bypass and early population exposure to fission and activation products. Analyses at AECL points to a potential failure of a fuel channel instead of a bunch of boiler tubes. There is ample data to dispute that outcome. Any uncontrolled rupture due to over pressurization at this stage is an unfortunate outcome.

This unplanned rupture of the pressure boundary occurs long before there is any severe core damage and a benign outcome that can be terminated by ECC, transforms into a serious accident whose economic consequences can be prohibitive even if a subsequent mitigation, for example by ECC injection upon this forced depressurization, is successful.

The uncontrolled failure can also be at any other location within the heat transport system. It could be in the pump and cause a containment bypass at Bruce. Were it to occur at a fuel channel the effects can be catastrophic economically as a high pressure incore rupture can cause extensive damage to other channels and in-core devices. Onset of a severe core damage is likely accelerated by draining the moderator with a potential end fitting ejection following a channel rupture.

With boilers no longer a heat sink, gradual voiding of individual fuel channels and sequential onset of fuel heatup in the 480 fuel channels (depending upon individual feeder size and channel power) leads to heatup of the heavy water moderator and light water in end shields and shield tank.

A voiding of the Calandria vessel occurs as rupture disks cause partial moderator expulsion upon onset of boiling. The fluid expulsion may be smaller than previously modelled, yet an avoidable artifact. A properly designed relief valve on the moderator could delay onset of severe core damage.

A high pressure injection of water into PHTS is not available and there is no way of manually depressurizing the heat transport system. Inventory in the reactor continues to deplete.

An initial high pressure failure of an overheating channel into the moderator can also expel a part of the liquid moderator by carryover if the initial overpressure induced failures in boiler tubes rupture just enough tubes to relieve the stresses but maintain high PHTS pressures. A properly designed PHTS relief valve would also maintain high pressure in the system and an initial high temperature failure of a fuel channel at high pressures cannot be precluded. Combined with other design changes accident can be easily manoeuvred to end favourably but not so in the current design.

*Overheating channels (*Figure 4*), fed by steam circulating through the heat transport system also contribute to a natural consequential heatup of downstream end fittings and feeders. Different channels void at different times depending upon their decay power and volume of water in their feeders.*

With some channels exposed following moderator depletion and losing all significant heat sinks, conditions form for accelerated fuel bundle overheating, deformations and bundle dissociation at low pressures. For all channels, the downstream end fittings and insulated feeders start oxidizing upon heatup by high temperature steam exiting channels. An early breech of a channel within the moderator space creates path for interaction of moderator water with dry channels and for a long time thereafter steam is supplied by the underlying moderator for fuel bundles and feeders to oxidize.

Figure 5 illustrates channel power distribution in the reactor. The high power channels typically heatup and disassemble early but the low power channels may contribute more to Deuterium gas production in their feeders. The channel heatup is accelerated as moderator depletes and uncovers rows of channels. Channel segments begin to disassemble and supported by underlying channels and constrained by in-core devices continue to cascade down and heatup during holdup periods.

Internal sources of water remaining in the end fittings, pump inlets, fuelling machines also contribute to oxidation of fuel and feeders. The pressurizer location in Bruce reactors is below headers and the volume of water contained in the pressurizer will affect the accident progression by supplying water during slow depressurization transients.

Flammable gas production from carbon steel oxidation may well exceed that from Zircaloy oxidation, especially for low power channels that do not disassemble but continue to circulate dry steam and oxidize the feeders over a long period of time.

With no pressure vessel to completely isolate the hot fuel from the containment, the overheating fuel & channel debris heatup further and their uncovery in steam over next few hours results in a direct expulsion of un-attenuated fission products into the containment. Figure 8 *shows that the fission product release may overheated fuel may be fastand release of large fraction of fission products into the containment inevitable. Containment integrity becomes an important safety concern. Fuel sheath failures cause the free inventory of fission products to release followed by diffusional releases from grain boundary and grain bound species. All fission products find an easy path to the reactor building (not to be confused with the traditional containment that regular single unit PWR and PHWR reactors sport). Releases to the environment, accounting for settling and re-volatilization inside the building, depend upon time at which building failure is initiated.*

Bruce reactors will have special issues with capture of flammable Deuterium in the reactor vaults. The gas production by oxidation of fuel and feeders will occur after the vacuum building has cycled to reduce the containment pressure. As the containment pressure settles to just over atmospheric pressure and intra compartmental air flows subside, the release of Deuterium into the reactor vault will occur through the Calandria vessel rupture disks. The flammable gas will tend to accumulate inside the reactor vault (free volume per reactor vault only about 15% of the total free volume, Figure 2*) and reach very high local concentrations. Some gas will escape into the top of the deck where* *no hydrogen mitigation measures may exist (as mechanical failures of deck level seals in-core devices lost in the core disassembly process cannot be precluded).*

Analyses confirm that the whole CANDU core cannot just fall down after a certain amount of debris have formed. The erstwhile MAAP-CANDU assumption of a 'core collapse' is a convenient way of decreasing source term to please ourselves. It is the channels that do not fail that contribute most to hydrogen source terms, analyses now reveal. A large number of fuel bundles (~33%) may remain in stubs at the end of channels that do not experience rolled joint pullout. Oxidizing feeders in channels that disassemble will cool down relative to feeders in channels that remain intact.

*At Bruce there is no pressurizable containment as the reactors are housed in quasi industrial buildings (design pressure < 70 kPa(g)= 70% of 1 bar gage (1 atmospheric pressure over normal)) built to National Building Code and CSA N287.4. Pressure suppression and pressure limitation functions are left to a single vacuum building. It is not even clear if a severe accident in one unit can be handled by the reactor vault (*Figure 2*) and vacuum building with major focus on hydrogen trapped in the reactor vault for a single unit accident. A more realistic evaluation of severe accident progression for Bruce reactors is pending, especially for a multi unit accident. The reactor building envelope has a relatively low failure threshold for over pressure (less than 1 atmosphere; buildings are supposed to be tested every six years at 115% of design pressure according to R-7 but this requirement is often deferred as in the case of Darlington at test anniversary of 2009). The acceptable leakage rate is a value agreed upon between CNSC and the utility and at 2% mass fraction per hour at design pressure is about 500 times more than that for a typical PWR (0.1% / day volume fraction*), see Figure 3 .

Given the large amount of Zircaloy in reactor channels and carbon steel in the CANDU feeder pipes, stainless steel in end fittings and vessels, accelerated Deuterium gas releases into the containment readily exceed the local detonation limits as the small number of passive recombiners, where present and interactive to the stream of combustible gas, are not only unable to arrest the increase of deuterium concentration but also introduce additional ignition potential leading to gas detonation at concentrations above 5 to 6%.

*The reactor vaults will receive from the disassembling reactor core and hold flammable deuterium gas with little reason for the gas to distribute to the vacuum building connected from below the reactor vaults (*Figure 2*) . Leakage of Deuterium to the confinement space above the reactor deck cannot be precluded especially through the seals around pump and boiler penetrations and the reactivity mechanisms. Burn/detonation of Deuterium mixtures in the confined space under the reactivity deck is facilitated by high local temperatures and confined spaces.*

Early breech of the confinement pressure boundary by simple overpressure pulse by just above 1 atmospheres cannot be avoided.

The debris formation in a CANDU reactor is in solid chunks of channel and its eventual retention upon 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 thus introducing water from the shield tank onto hot debris.

The effect of Calandria vessel weld failure can vary from additional hydrogen production, accelerated FP releases as one mode of outcome to catastrophic vessel failures by energetic interactions with the hot and molten solid-liquid debris at the bottom of the Calandria vessel as the other mode.

Shield tank relief valves cannot remove decay heat equivalent in steam as they are designed for a smaller gas relief capacity. An onset of boiling in the shield tank has a potential to cause it's failure.

Reactor building failure at any one of 2-3 different events coincident with energetic interaction of fuel and water is possible. Multi unit reactor accidents will cause an earlier containment failure.

Vacuum building acts to reduce the overall pressure rise but cannot pressurize to any significant levels beyond a single atmosphere above normal (design pressure ~ 0.5 atm).

Here is a rehash of phenomenology and design features that affect consequences:

1. *As soon as the boilers dryout, the primary heat transport system at Bruce will repressurize and an uncontrolled rupture of the pressure boundary will occur because the PHTS over pressure relief valves are far too small to handle decay heat at boiler dryout of about 30 MW. If the rupture is in a channel the shareholders are in for a billion dollar surprise even if the ECC system actuates (best case scenario) and further progression of accident is avoided. If instead, the ever so vulnerable boiler tubes burst to relieve the excess energy and ECC does not come in (worst case scenario) a most undesirable containment bypass occurs and public is potentially exposed to un attenuated releases from overheating fuel in 480 fuel channels gradually and sequentially running out of water. Bruce power liability and damage to environment becomes unfathomable. See page 18 for a partial discussion of the over pressure protection issue that has remained unresolved for 14 years and has included 10 years of OPG/Bruce Power misinforming about relief valve capacity and 5 years of accepting that error in judgment and now maintaining a position that a channel rupture is an acceptable outcome. Combined with an inability to manually depressurize the system (as PWRs can) or add emergency coolant at high pressures, a potentially benign event of a loss of power is turned into a reactor damage accident. Fix is in replacing two $38k valves that are not only inadequate but termed 'bad actors' by internal Bruce Power Opex .*
2. *As the fuel in the channels begin to heatup so do the end fittings and feeders. Oxidation of feeders starts at about 550 C while fuel oxidation starts at about 800 C. Over 10 km of carbon steel feeders provide over 2000 m^2 of carbon steel surface area for oxidation. Carbon steel oxidation to $FeO/Fe_3O_4/Fe_2O_3$ (in 95/4/1 ratio of Wusite, magnetite and haematite) is faster than that for Zircaloy at the same temperatures and the iron oxides*

have a propensity to peel off and expose fresh steel carbon surface for accelerated oxidation. Stainless steel end fittings also join in the oxidation process, albeit at a rate that is at times 10 times slower. Part of end fittings also include a heat sink to the end shields. Heatup of feeders will likely start fires in the feeder cabinets.

3. *As channels use the moderator to reject the heat, the moderator begins to boil and its rupture disks actuate in absence of an adequate relief system. Core uncovery is accelerated and Calandria tubes and pressure tubes begin to deform, sag and initiate cracks. This exposes the internals to steam produced in the calandria vessel. Parts of channel disassemble, copious amounts of flammable deuterium gas are produced from reaction of steam with Zircaloy in fuel, pressure tubes and Calandria tubes. More deuterium (isotope of hydrogen) is produced by intact carbon steel feeders than by intact fuel bundles. This has been confirmed by analyses using a new computer code ROSHNI.*
4. *Feeder oxidation is exothermic (gives out enormous amounts of heat) and the heatup initiates fires in the feeder cabinet insulation. This also triggers burns and explosions of the heavy hydrogen generated in the channels and released from failed channels into the calandria vessel and ultimately into the small reactor vault. Accumulation and concentration of flammable gas inside the individual unit reactor vaults is very likely with local concentrations of deuterium exceeding flammable concentrations easily.*
5. *The relatively small vacuum building is unable to maintain low pressure and reactor building fails in response to energetic interactions of water with debris and hydrogen explosions.*
6. *A part of the overheating and disassembling core makes it to the bottom of the Calandria vessel. A large number of low power peripheral channels do not fail and attain temperatures that continue to cause oxidation of fuel and feeders but avoid gross failures.*
7. *Inevitable failure of thin walled Calandria vessel will cause water from the shield tank to energetically react with debris and cause structural failures in these vessels as well as the containment structure mechanically joined to them and just overhead.*
8. *Large releases of activity into the environment are inevitable.*
9. *Opportunities to arrest the progression of accident early can only be availed by significant investment into understanding the accident progression and instituting design changes to incorporate intelligent recovery actions.*

‘HYDROGEN’ ISSUE

This issue should have been addressed 20 years ago for design basis accidents. The oxidation potential of feeders as significant sources of flammable Deuterium / hydrogen gas was never addressed. Thus the hydrogen mitigation measures designed for under 100 kg of H_2 based solely on partial oxidation of Zircaloy sheaths would never be sufficient for the ‘hydrogen’ that can be generated by oxidation of carbon steel feeders by steam for LOCA+LOECC scenarios as well as severe core damage accidents.

Commissioners should look first at the design based accident analysis submissions by Bruce power and ask the simple question of why extensive fuel heatup under LOCA + LOECC scenarios is predicted as anticipated but never is the thermo-chemical behaviour of end fittings and feeders analyzed.

My analysis shows that carbon steel feeders produce enough flammable deuterium gas for a sustained LOCA+LOECC scenario lasting many hours to make the Zircaloy source deuterium look inconsequential. Also, please ask why the whole safety report never acknowledges difference between deuterium (D_2) production and hydrogen (H_2) production in a reactor that is cooled and moderated by D_2O. While you are at it, also ask why with a factor of 2 differences in transport and combustion properties, is the lighter hydrogen assumed to be same as deuterium in almost all Bruce and other CANDU submissions. Last time such a question was raised publically by a Commission member the response from a staff member was totally wrong when it was asserted that no differences exist between 2 gases. Ignorance is such a blissful state of mind.

For severe accidents, a comprehensive deuterium gas source term has never been determined as well. The severe accident computer codes in use (e.g. MAAP-CANDU) have no consideration of heavy water. They use light water properties and only consider H_2 production, not D_2 production just as the ability of PARS to mitigate it. After all PARS are first designed and tested for lighter hydrogen, not heavier deuterium. Do not let them tell you as in a previous public meeting that the two gases are the same in combustion and recombination. They are not. At least a hundred scientific papers attest to that. Deuterium would recombine at least 41% slower and burn quite differently. At a previous CNSC public meeting a CNSC staffer quite smugly and with a straight face mis-informed, hopefully only in ignorance, the commission about the gases being of identical behaviour.

Bruce safety report will confirm to you that for larger breaks fuel bundles as well as the feeders are hotter earlier and longer as ECC fails to inject (see Figure 4). These will produce more combustible deuterium. The small (65 kg, if I recall correctly) source term ‘hydrogen’ for LOCA+LOECC in the safety reports is amusingly wrong. Bruce power should amend estimates of that ‘design basis’ risk before being granted a licence extension. They should also provide a ‘hydrogen’ mitigation system that does not cause explosions beyond 6% hydrogen concentration as the current AECL PARS do. AECL has done experiments showing explosions caused by PARS and this was made public at last year’s CANSAS conference organized by KAERI at CNSC. I am sure the good engineers at AECL can come up with better PARS (alternate designs already available) or the industry as a whole can come up with a better hydrogen mitigation option than the current PARS that are so poorly suited for CANDU reactors spewing large concentrations of ‘hydrogen’ into the relatively small and congested reactor vault.

For severe accidents, the estimates of accident progression and hence deuterium production cannot be adequately undertaken by the computer codes currently available to the Canadian industry. There are far too many errors and omissions in the code MAAP-CANDU that they use now. These have been presented to the industry many times; last about a year ago at CNSC. None have been fixed.

Installation of Passive Autocatalytic recombiners (PARS) has become an acceptable hydrogen mitigation system for severe accident because of their passive action, relatively well understood phenomenology, start-up at low hydrogen concentrations, efficiency under both beyond-design-basis and design-basis accident conditions, and implementation that does not constrain normal operation.

Yet, there are three issues that must be considered:

1. The PARS units should be sufficient in number and placement to avoid a hydrogen burn (limit hydrogen concentration to less than ~4%). Tests have shown that at any concentration greater than 5%, these units with a washcoat layer of the catalyst exude flames. There are other designs of catalytic plates that do not have this problem as by limiting the recombination rate the maximum substrate temperature is limited to below the auto-ignition temperature of hydrogen (Figure 7). At 6% hydrogen concentration they cause explosions. With such performance characteristics, no PARS are better than these PARS if the hydrogen concentration cannot be guaranteed to be kept well below 4%.

2. The PARS units should be qualified (sized and tested) for the actual flammable gas (deuterium in CANDUs) and not just for simple hydrogen. Data show that processes that dominate recombination by a catalyst maybe slower by a factor of up to $\sqrt{2}$ for Deuterium (reference 4). None of the installed units were tested for Deuterium. They were tested for common, lighter Hydrogen. CANDU severe accidents result in production of Deuterium first and predominantly so. CNSC staff do not know that as evident from a previous response[6] from them to an intervener.

3. PARS units should not cause a containment failure by the heat of recombination reaction or by the fires potentially caused by the high temperature gases exiting the PARS units. The recombination kinetics for hydrogen is;

[6] A response from CNSC to a question regarding Deuterium vs. Hydrogen in an email states "*While there has not been to our knowledge any demonstrated issue associated with deuterium versus hydrogen in the PARS, we are of the view that it would be at most a minimal concern given that the scenario where the PARS is needed assumes a severe accident where the heavy water coolant has been lost and is being replaced with emergency cooling water (which is light water).*" What an interesting (and patently wrong) understanding of when and which flammable gases are produced in a CANDU severe accident. Again it would be funny if it was not painful to realize that certain guardians of our nuclear safety know so little about severe accidents in reactors they are paid to regulate and that they are still allowed to hold their jobs. The email was copied by the CNSC author to the highest CNSC senior management. I wonder if the CNSC management (1) laughed silly as I did; or (2) smirked in knowledge that another intervener was smugly silenced with arbitrary answers; or (3) could not tell the difference between Deuterium and Hydrogen gases as well; or (4) were some of the original authors of this amazing revelation for which they would be laughed out of any high school chemistry class discussing the accident progression.

$$H_2 + 1/2O_2 = H_2O + 240 \text{ kJ/mole of } H_2$$

A 1 kg/hr removal of hydrogen by PARS is, from the above, equivalent to ~33 kW introduction of heat into the containment. An addition rate of about 10 MW heat can be anticipated for removal of hydrogen produced in a severe core damage accident when the correct number of AECL PARS units (~75 in a CANDU 6 building) are installed. This energy addition is enough to fail the containment by overpressure or potentially cause fires if the PARS are operated in high H_2/D_2 concentrations. If recombined with oxygen in a recombiner, only the hydrogen from steam oxidation of Zircaloy in a CANDU 6 reactor will produce over 225 GJ of energy (equivalent to 110 FPS, 3 hours of decay power at 1%). PARS units at a Bruce reactor, if properly sized and populated, will produce about 25% more per reactor unit.

The issue of recombiners requires a serious re-evaluation but this must wait until a more complete source term for deuterium gas has been established for Bruce reactors. Given that at present their analyses do not include feeder oxidation, any ‘hydrogen’ source term Bruce Power have is likely incomplete. This is an important safety concern and no license extension should be granted unless the issue is properly addressed.

PHTS OVER-PRESSURE PROTECTION ISSUE

None of the over pressure protection systems in the heat transport system, moderator or the shield tank are sufficient to remove decay heat when other means of heat removal are not available following an accident that may lead to severe core damage. Of primary concern is the over-pressure protection in the heat transport system.

After about 13 years of review of the issue of inadequacy of relief capacity of the over pressure protection safety relief valves, CNSC has now accepted the Canadian nuclear industry position that the steam relief capacity does not have to be sufficient to remove the thermal load (decay heat) and an uncontrolled rupture of the reactor pressure boundary is an acceptable outcome. After insisting erroneously for 10 years that the safety relief valves were properly sized for decay heat removal, it is claimed now that the rupture will most likely occur in a fuel channel once the boilers dryout and the relief becomes the sole heat sink. If the uncontrolled rupture were, however to occur in the boiler tubes, the resulting containment bypass can have catastrophic consequences and needs to be reviewed further now.

Bruce CANDU over pressure protection on the main heat transport system (HTS) is atypical of pressurized water reactors. (the fact that the design is atypical is not the issue but that the over-pressure mitigation capability of the implemented design is inadequate upon a loss of heat sinks). Instead of being a direct and unobstructed relief path as required by the ASME code, section III, NB-7141 (b) - it is composed of two sets of valves in series (Figure 9), separated by a small low pressure vessel called the bleed condenser. The first set of valves are typically called Liquid Relief Valves (LRVs) and the second set of valves are called Safety Relief Valves (SRVs), although both sets are designed in CANDUs for a certain liquid relief with a small steam relief capacity, typically also not certified. Under conditions of boiler heat sink termination, these valves must pass enough steam to match that produced by decay heat, in order to avoid an over pressure.

This is an uncommon arrangement that can work if both sets of valves open when required and adequately relieve the excess energy thus maintaining the pressure in the HTS at levels that are safe. Canadian AECB regulatory document R-77 defines ‘safe’ as 10% overpressure for events that are frequent and 20% for rare events. In no case is any over pressure protection system allowed by ASME Boiler & Pressure Vessel (BPV) code to permit a failure of the pressure boundary. Strict rules exist for ensuring, by pre-installation testing, that the valves would function as required under extreme conditions. NRC even insists on periodic certified steam relief capacity testing of the installed safety relief valves, something that CNSC apparently does not.

The design relief capacity of the over-pressure protection SRVs at Bruce is ~1.5 kg/s of steam at ~10 MPa per valve. Both sets of valves are essentially specified for liquid relief, typically based on a D_2O bleed closed with D_2O feed full strength in. Steam relief capacities are improperly specified as very small values, with perhaps the expectations that the design basis does not include passage of steam. Compare the 3 to 4 kg/s steam relief capacities of the two SRVs to a reference value of ~20 kg/s as the decay heat equivalent for a Bruce reactor at the time of boiler dryout under a station blackout scenario.

The design value of the steam relief is inadequate just by inspection. It was easily shown by application of a simple ASME equation on the actual valve geometries (tested flow area of about 35 mm^2 in steam) that the SRVs can never discharge enough steam (Figure 12) to avoid an overpressure. It was also shown by some AECL testing at Wylie Labs & valve spring analysis that the valves cannot open fully under steam conditions (lift of about 1mm out of a total possible lift of 4mm) and thus are only able to relieve less steam than needed. A proper over pressure protection will not be available when required. This can result in an uncontrolled rupture of the pressure boundary.

So a serious safety problem arises if the safety relief valves cannot relieve enough steam or if one or more of them fail to actuate when required to do so. Good designs provide redundancy and adequacy. In case of a station blackout scenario (loss of all AC power) the derived engineering requirements on the overpressure protection system are exactly the same for all reactors worldwide – **remove excess energy by steam discharge equivalent to decay heat by actuating passively and reliably and avoid an over-pressure**. These requirements are easy to quantify and understand.

Decay heat at boiler dryout is typically about 1% and for a Bruce reactor that is about 25 MW or 25 kg/s of steam equivalent. For a larger PWR that is about 30 MW equivalent to about 30 kg/s of steam roughly. The US PWRs typically have 5 SRVs with an ability to remove up to 250 kg/s of steam resulting in an ability to maintain the poressure in the system at the set point of the safety relief valves (Figure 10), while the CANDU steam relief capacity from 2 SRVs is capped at 4 kg/s will result in an uncontrolled rupture (Figure 11). It is not that the US PWRs need to relieve 250 kg/s. They would never need to relieve any more than 30 kg/s steam after a SBO but the redundancy and adequacy of steam relief is result of the good engineering practices in design and safety margins. The difference in relief capacities of 6000% with CANDUs is alarmingly high with the difference in core thermal power relatively small, ~30%.

The subject valves in all CANDUs replaced properly designed valves in 1996 when the industry panicked after the relief valves chattered and stuck open at Pickering and caused an unprecedented ECC actuation.

Again, the safety concern is as follows. If the SRVs cannot relieve the heat load when required and a resulting overpressure causes the vulnerable boiler tubes to fail then the release of activity through the open Main Steam Safety Valves (MSSVs) will cause a containment bypass and an undesirable exposure of public to activity contained in the steam. If fuel failures follow, the resulting exposures can be catastrophic. If the accident happens at Pickering, parts of Toronto will suffer greatly and immediately. The issue therefore is not frivolous but the response of the industry has certainly been so. The valves cost $38k each.

The SRVs are spring loaded valves whose claimable capacity to relieve a certain flow rate of liquid and certain specified flow rate of steam is required by ASME code to be certified by tests. CNSC has not understood this simple requirement or required the licensees to produce results of such tests.

ASME Boiler and Pressure Vessel Code, section III, NB-7000 requires that SRV fluid (steam or liquid) relief capacity be certified by tests and only tests. From information made available by the licensees to CNSC, it is apparent that none of these replacement valves for any of the CANDU reactors were most likely tested properly for any service and were definitely never certified for steam relief (an examination of the test data indicates that even liquid relief capacity tests did not meet the 5% scatter rule). A small number of tests for liquid relief for Bruce/CANDU 6 type valves at Wylie labs did not fully conform to the ASME testing requirements either. However, the design capacity of 1.5 to 2 kg/s for steam discharge were indicated by sample tests performed by AECL on Bruce like SRVs at Wylie Labs.

The following is a summary of the SRV test requirements that should be all followed by CANDU licensees:

1. *The actual safety relief valves must be tested individually in steam at representative conditions in a certified facility. Tests are mandatory and cannot be substituted by a computer models unless verified by test data for the same geometry of valves.*
2. *Installation geometry must be replicated in tests.*
3. *Three to four valves are to be tested (number depends upon the method used to certify relief capacity). Three discharge tests per valve are required.*
4. *Test data on Opening Pressure or the Set Pressure (pressure at which the valves open to sustain a discharge) must fall within 3% of the design value.*
5. *Rated discharge capacity must be attained within 110% of the set pressure.*
6. *Inlet pressure losses on valves as installed be no more than 3% (non-mandatory)*
7. *Any valves that give a relief discharge more than 5% from the average must be rejected.*
8. *Effect of uncertainties in measurement should be considered.*
9. *Only 90% of the average tested relief capacity is used as certified relief capacity.*
10. *Maximum possible steam discharge can be pre calculated using Napier equations and their corrections for superheat and pressure. A coefficient of discharge equal to the ratio of the actual flow to the maximum flow is developed and used.*
11. *Extrapolation or proration to a pressure higher than the pressure at which the relief capacity has been certified is permissible by the ratio of pressures. So at a pressure greater by 20% over the certification pressure, the relief capacity can be claimed to be greater by only 20%.*
12. *Extrapolation to other fluids is according to Section XI of the ASME code. Steam service valves should always be tested in steam.*

Safety Relief valves are required in all pressure vessels when there is a mismatch between heat generation and heat removal. In a Station Blackout Scenario in any nuclear reactor including CANDUs, that occurs when the boilers run dry. At that time, in absence of another heat sink the fuel decay heat must be removed by the SRVs to avoid an over pressure. If the SRVs are properly sized they would relieve the decay heat load as equivalent amount of steam and maintain the system pressure at about 10% above the operating pressure. In a CANDU reactor the decay heat at boiler dryout may be about 1% of the total original thermal heat production. In a Bruce reactor that is about 25 MW or about 25 kg/s of steam equivalent. Adequacy of the SRVs has been demonstrated in all reactors except operating CANDUs. The 250 kg/s of relief capacity at a PWR does not mean that the actual relief is 250 kg/s. it just means that the relief will balance production of steam.

If the safety relief valves cannot relieve decay heat energy by steam relief, as is the case in CANDU reactors where the total SRV steam relief capacity is about 4 kg/s at opening pressure against about 20 kg/s of internal steam production, system pressure will rise, steam discharge rise and if inadequate will cause the pressure to rise uncontrollably such that some component will eventually rupture. ASME BPV codes are formulated to avoid this outcome and it is an ASME requirement for Class 1 components that SRVs be properly sized and tested. This includes testing of the actual valves to certify whatever fluid (liquid and/or vapour) relief capacity needs to be credited. In a Bruce reactor a certified steam relief capacity of at least 25kg/s (from one valve if the usual single failure is accounted for, otherwise from 2 valves) will insure that the energy relief will be sufficient to balance energy production when boilers run dry. A larger relief capacity as in all LWRs will not cause a larger overall relief. The relief will never average more than production.

It is clear that the subject valves, replacing a properly designed valves in 1996, are ill designed for ALL CANDU reactors and their designer specified steam relief capacity of ~1.5 to 2 kg/s of steam is just not sufficient to remove energy production at the time when they are required to work. The subject Bruce SRVs were actually designed for **liquid** relief of about 27 kg/s and a steam relief of 2 kg/s. Tests showed that these valves lift fully under liquid relief conditions but lift only partially (20%) under steam relief conditions (thrust force by steam on valve seat is significantly lower than for liquid water). The discharge area is proportional to lift and is significantly smaller for steam. This was confirmed by testing and actually an engineered valve spring feature to meet the design specifications of 1.5 to 2 kg/s of steam discharge capacity. The reactors must enhance the over protection system by installing safety relief valves that preclude a pressure boundary failure. AECL confirmed the inadequacy of the steam relief capacity (Figure 13) in analyses presented in 2011.

The fact that the PHTS over pressure protection by the bleed condenser relief valves is inadequate is well established. What is also well established is that the industry, including Bruce Power misinformed about steam relief capacity for 10 years and the CNSC staff assigned to the task were unable to check the facts using a simple equation. It was only 10 years later in 2011 that AECL finally admitted in public that the submissions from the industry on the critical steam relief capacity were wrong and an uncontrolled over pressure induced failure is an inevitable outcome. CNSC has done nothing since then to fix the problem and has now accepted an undesirable outcome of an uncontrolled over-pressurization of the heat transport system and failure. It is claimed now that the fuel channels are the weakest link and would fail, ignoring the fact that it is a terrible outcome (what if an end fitting is ejected and the moderator drains? Etc.) This disregards available evidence on vulnerability of boiler tubes. An attempt was made to discredit the issue using an outside consultant who made no effort to justify the low steam relief capacity but took issue with the language used by the intervener. CNSC has let this important issue fester and considers the issue closed. It will not go away by wishful thinking. Given how this has been handled for 14 years, itt just makes them look petty, uncaring, unresponsive and technically challenged. I will be happy to provide further details and failing a clear resolution I am planning on bringing this up in an important international forum this summer.

If CNSC members cannot collectively understand the importance and gravity of this simple technical problem as both a safety issue and an economic issue for the utility, then the whole regulatory regime will have to be publically re examined.

SUMMARY OF BRUCE A/B SEVERE ACCIDENT PROGRESSION & MITIGATION ISSUES

- Bruce A/B reactors did not consider severe accidents in the design process. Unreasonable to expect easy severe accident mitigation.
- Severe accidents in all inter-connected units a nightmare scenario.
- Current Bruce A/B designs inherently forces a reactor damage even before an ECC loss leading to severe core damage.
- No provisions for manual depressurization after SBO. No super high pressure ECC or makeup intervention / injection.
- Onset of a severe core damage in a CANDU reactor puts activity directly into the containment. There is no holding of activity in a vessel like in a PWR pressure vessel.
- Significantly higher sources of hydrogen from large amounts of carbon steel and Zircaloy. Recombiners will cause explosions.
- Enhanced potential for energetic interactions with enveloping water
- Pressure relief in ALL relevant reactor systems in inadequate (PHTS, Calandria, Shield Tank, Containment)
- Bruce containment – a negative pressure concept - amongst the weakest in the world for pressurization; severe accidents will cause pressurization
- Containment bypass from reactivity device failure a likely outcome after a severe core damage
- Calandria vessel cannot contain debris and can fail catastrophically at welds.
- Shield Tank cannot contain pressure upon boiling and can fail. Restoration of cooling after water depletion problematic as flow outlet at the top of vessel.
- Inadequate instrumentation and control.
- Poor equipment survivability
- Currently planned PARS inadequate and potentially dangerous.
- 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.
- Current SAMGs are inadequate. Many Emergency hookups not implemented
- High risk potential from external events
- Need to reconsider malevolent actions and sabotage.ent bypass from reactivity device failure a likely outcome after a severe core damage

QUESTIONS THAT COMMISSION MEMBERS MUST ASK BRUCE POWER TO PROVIDE ANSWERS TO

A licence renewal affects all units including those that would undergo refurbishment. Therefore, there are THREE main issues as far as severe accidents are concerned (see A , B, C below). Any licence renewal should be subject of satisfactory resolution of the following set of questions as adjudicated by an independent panel of experts.

A. WHAT ARE THE SEQUENCE OF EVENTS AND CONSEQUENCES OF A SEVERE CORE DAMAGE ACCIDENT LIKE THAT AT FUKUSHIMA IN WHICH ONE OR ALL CURRENTLY LICENSED AND OPERATING UNITS ARE AFFECTED BY A LOSS OF AC POWER. GIVEN THAT THE UTILITY SUBMISSIONS ARE MISSING THE NECESSARY INFORMATION, CAN THE UTILITY PROVIDE INFORMATION ON ANALYSES PERFORMED TO DERIVE REACTOR CONDITIONS AS A FUNCTION OF TIME, SOURCE TERM TRANSIENTS AND THE CONSEQUENCES THEREOF. WHAT NEW MEASURES ARE IN PLACE NOW FOUR YEAR AFTER FUKUSHIMA TO DEMONSTRATE THAT THE UTILITY CONSIDERS SEVERE ACCIDENTS SERIOUSLY AND THAT CONCRETE STEPS (NOT PLANS TO MAKE PLANS AS REQUIRED BY THE CNSC FUKUSHIMA ACTION ITEMS) HAVE BEEN TAKEN TO :

1. Further reduce the likelihood of a station blackout scenario that starts with a loss of off-site power or a malevolent act.
2. Reduce the likelihood of events and failures that create permutations of failures that may lead to severe core damage accident from other internal and external events
3. Reduce the likelihood of incidents progressing to a core damage state by measures such as external and internal hookups for adding power and water; daerator hookup.
4. Reduce the likelihood of an uncontrolled rupture of heat transport system pressure boundary at the onset of boiler dryout in case of a station blackout as at Fukushima.
5. Correct the inadequacy of heat transport system over pressure protection
6. Reduce the likelihood of containment bypass in boilers
7. Reduce the likelihood of containment failure by pressure, temperature, radiation and fluid/gas interactions with containment penetrations given that certain reactor units have weak confinement structures and no pressurizable containments.
8. Evaluate and document the effect of recovery actions including power restoration, water injection as a function of time since onset of core damage
9. Install additional and independent of that available before Fukushima, instrumentation to detect and help control the progression of a severe core damage accident
10. Reduce likelihood of recovery actions exasperating the accident consequences by enhanced severe accident specific instrumentation and display of state of the reactor
11. Reduce likelihood of fuelling machine adversely affecting the outcome upon restoration of cooling functions

12. Modify Calandria vessel overpressure system to avoid fluid loss through rupture disks; delay onset of severe core damage
13. Modify moderator cooling system to install recovery system hookups for inventory replenishment and reinstatement of cooling functions
14. Investigate potential of in-situ design enhancements to avoid Calandria vessel failure by hot debris to avoid catastrophic failure of reactor structures
15. Increase the likelihood of successful external water injection by manual depressurization of the heat transport system
16. Increase the likelihood of core inventory degradation by ultra high pressure water addition to pressurized HTS before core degradation and prior to an in-core rupture
17. Increase the likelihood of reactor heat transport system heat removal by thermosyphoning by adding systems to remove non condensable gases that can degrade thermosyphoning
18. Reduce the likelihood of ECC injection failure
19. Modify shield tank over pressure protection system to conform to anticipated heat loads to avoid catastrophic failure of shield tank vessel.
20. Install hookups for water addition to the shield tank
21. Obtain a more realistic evaluation of accident progression by using analytical methods that are more modern than the MAAP4-CANDU code that is 25 years old and obsolete in light of new information; and model the event with :
    - More detailed modelling of reactor core by differentiating between different bundles by modelling all reactor channels and incore devices
    - More appropriate modelling by using D_2O properties
    - More appropriate modelling by evaluating Deuterium (D_2) gas production, transport, recombination and burns. Has the utility considered that Deuterium gas properties differ greatly from hydrogen (H_2).
    - Considers oxidation of end fittings and feeders as sources of flammable D2 gas during a severe accident
    - Consider a more representative inventory of fission products
    - Consider concurrent fires (e.g. In feeder cabinets) as core voids, heats up and degrades
    - Consider failure of Calandria vessel at welds with hot debris
    - Consider failure of Calandria vessel penetrations at the bottom of the vessel (moderator outlet)
    - Consider explosive interaction of water with melt in Calandria vessel
    - Consider explosions caused by interaction of deuterium gas with PARS
22. Consider alternate hydrogen mitigation measures as PARS may become ignition sources; consider upgraded catalyst plates with electrolytic deposition that limit gas temperatures.
23. Installation of measures to avoid ignition in existing PARS
24. Consider D_2 mitigation system optimization for a100% Zircaloy oxidation (also to include effect of feeder oxidation)
25. Consider enhanced deuterium concentration monitoring systems within containment and Calandria vessel
26. Consider advanced video surveillance systems
27. Consider measures for mitigation of consequential fires during the progression of core disassembly

28. Consider post accident monitoring system instrumentation and control survival and functionality for severe accident conditions
29. Consider emergency filtered containment venting for severe accident loads
30. Consider improvements to pressure suppression system in reactor building as the vacuum building may be inadequate to avoid building failure for multi unit accidents
31. Consider reactor building reinforcements to avoid building failure; special emphasis on confinement on top of reactivity decks in multi unit station
32. Consider deploying on-site and off-site radiation detection equipment that actually detects the source characteristics and differentiates between incident radiation species by measuring the energy of incident radiation; does not get saturated by incident particulates as happened for Chernobyl at Leningrad station a thousand km away.
33. Develop methods and acquire instrumentation to help deduce source terms from radiation measurements so that prediction of radiation effects can be made for different locations and changing weather conditions
34. Develop simulators to train the operators in progression of a severe core damage accident and develop experimental basis & analysis to help avoid potential adverse outcomes of various mitigation measures.

The list of design and operational enhancements must complement a plan for operator training and emergency preparedness.

B. IF THE LICENCE RENEWAL COVERS REFURBISHMENT OF ANY UNITS AT BRUCE SITE, THE FIRST QUESTION THAT NEEDS TO BE ANSWERED RELATED TO SEVERE ACCIDENT PREVENTION, MITIGATION AND CONTROL CAPABILITIES IS:

What specific standards have been set for severe accident related capabilities for new reactors at design stage and whether a gap report has been prepared or is required to be prepared for the reactor capabilities that would be instilled in the reactor units upon refurbishment.

All questions raised for operating reactors (see A above) also apply to any units in refurbishment plans. No licence renewal should be granted unless satisfactory resolution has been agreed upon at a public technical forum. It is hoped that mature and detailed design requirements and realistic risk targets will be developed by a competent authority for a new generation of Canadian nuclear reactors.

C. CNSC MEMBERS SHOULD LOOK FOR AND PROVIDE TO PUBLIC FOR REVIEW REPORTS ADDRESSING THE FOLLOWING FUNDAMENTAL QUESTIONS ABOUT RELICENSING

1. Does the aging plant still meet the original licensing basis using the acceptance criteria employed by regulators last time the plant was licensed
2. Has any new information changed the understanding of previously employed acceptance criteria within the original licensing basis
3. Does compliance with original licensing basis mean that risk from the original licensing basis is acceptable today
4. Has there been any relaxation of original licensing basis along the way
5. Has an independent, off-shore review of the licensing basis and its compliance been undertaken
6. Will the plant be licensable today in Canada and in other jurisdictions
7. Does/should the public have different expectations of risk today
8. Is it fair that plant be required to meet different public expectations
9. Should risk from accidents previously not considered in licensing basis be evaluated and has it been properly evaluated and acceptable today
10. Is the regulatory regime independent, impartial, competent, effective & relevant

I remain a proud CANDU safety engineer and the idealist in me trusts that these hearings will herald a new chapter in the deployment of safer reactors at Bruce; with the realist in me knowing better and fearing for those living close to Bruce reactors. I just wish, as I inch very close to retirement, that there was more honesty in matters nuclear and that national interests superseded flag waving about infallibility of our reactor designs. I wish the present regulatory regime improves and we update our operating reactor designs not only in interest of safety of fellow humans living close to them but also in interest of revival of CANDU industry and national development. Nuclear reactors are necessary for our present and future energy needs. People and institutions who hinder their safe deployment are not.

Sunil Nijhawan

Toronto 7 April 2015.

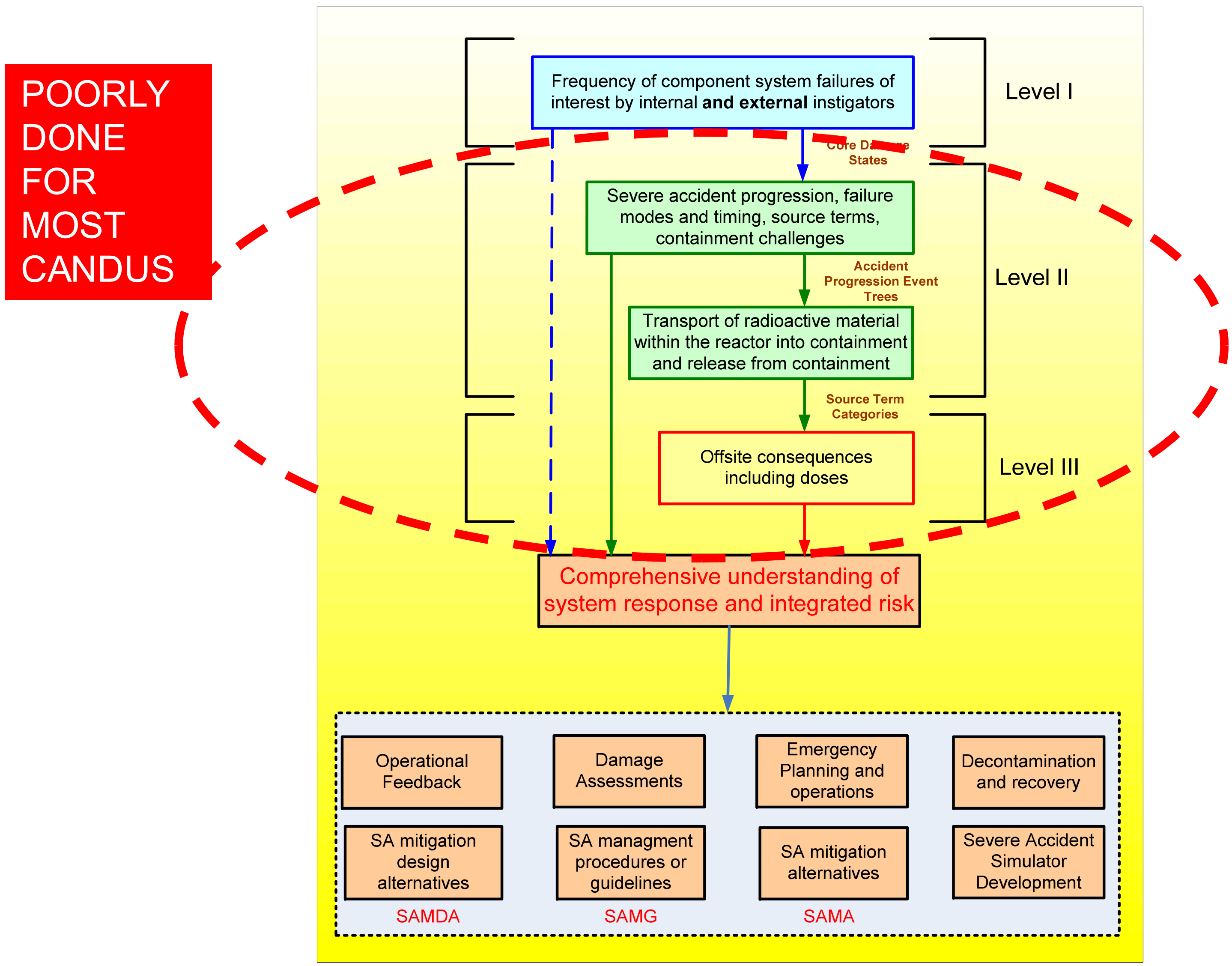
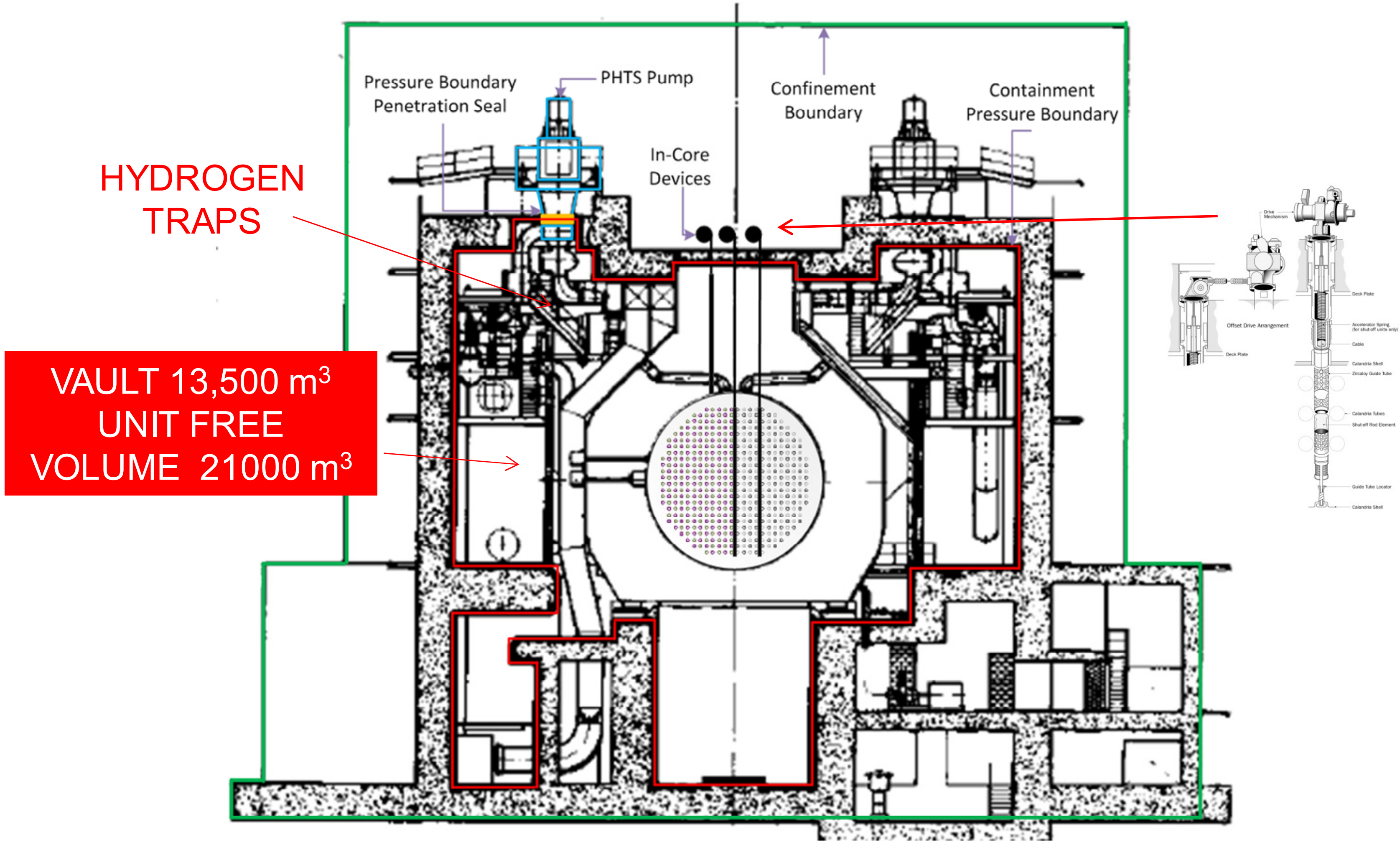


Figure 1 : RISK EVALUATION AND RISK REDUCTION PROCESSES



Total free volume 96,000 m^3 for 4 units, 69000 m^3 in vacuum building, max design pressure 48 kPa(g) at VB

Figure 2: CONTAINMENT IN SEVERE ACCIDENTS

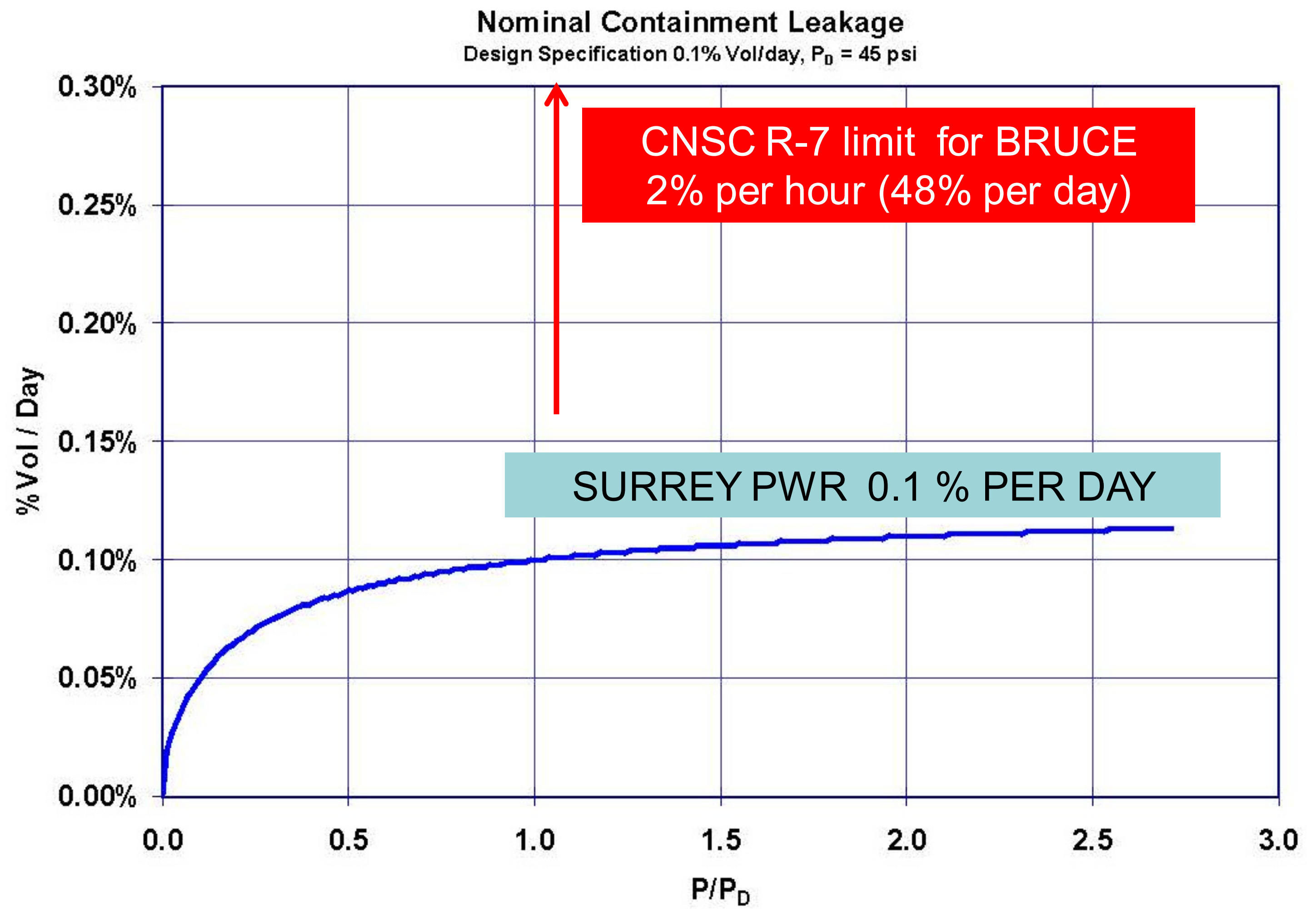
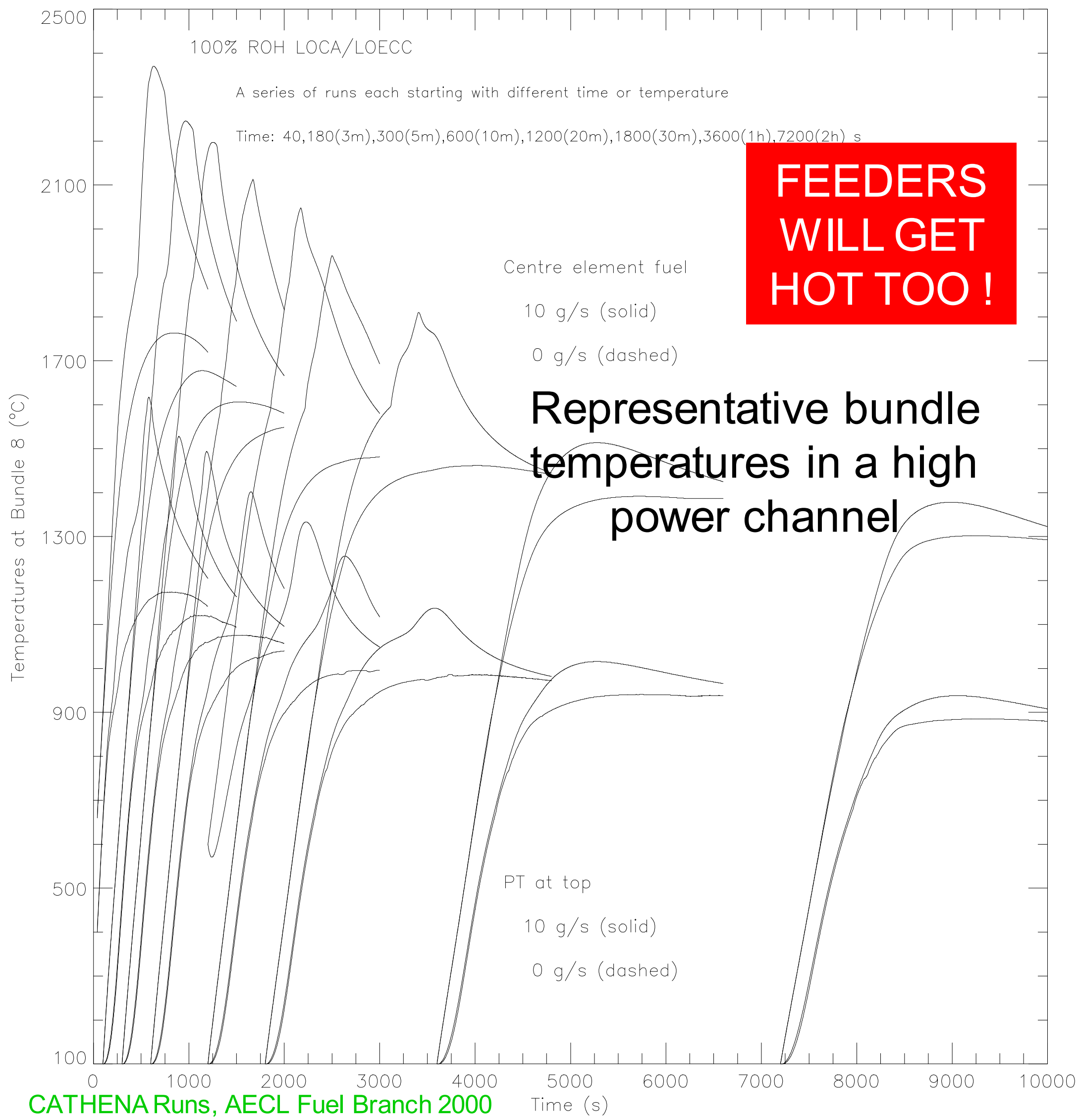


Figure 4-10 Nominal Containment Leakage Model Source : NUREG-7110

Figure 3: COMAPRISON OF PWR AND BRUCE CONTAINMENT ACCEPTABLE LAEKAGE RATES



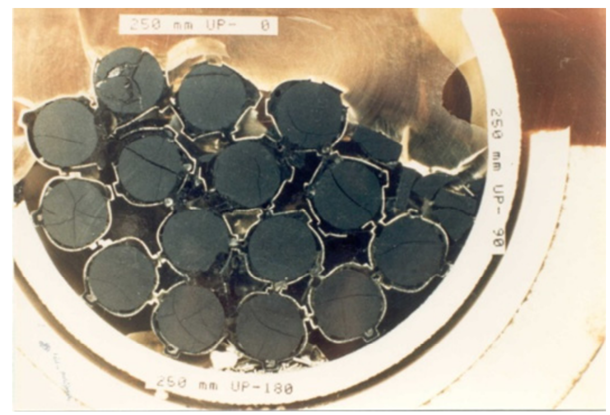


Figure 4 : Example of LOCA + LOECI fuel temperatures as a function of onset of fuel dryout

FEEDER SIZES THAT DEPEND UPON POWER HAVE A LARGE IMPACT ON TIMING OF FUEL HEATUP IN INDIVIDUAL CHANNELS

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
A								3620	3945	4240	4420	4463	4463	4419	4239	3945	3619							
B						3650	4210	4677	5038	5286	5426	5439	5438	5425	5285	5037	4676	4209	3649					
C					4036	4595	5159	5618	5883	6052	6132	6101	6101	6132	6051	5882	5616	5157	4593	4035				
D				4158	4831	5412	5856	6164	6095	6167	6170	6060	6060	6170	6165	6093	6162	5854	5410	4830	4157			
E			4041	4843	5579	6026	6305	6178	6230	6246	6192	6008	6008	6191	6245	6228	6176	6302	6023	5577	4841	4039		
F		3584	4571	5445	6036	6276	6137	6260	6329	6337	6262	6059	6059	6262	6335	6327	6257	6135	6273	6033	5442	4569	3582	
G		4125	4065	5804	6198	6011	6076	6279	6388	6415	6351	6153	6153	6350	6414	6386	6277	6073	6008	6195	5801	5062	4122	
H		4607	5432	6005	5990	5953	6023	6288	6437	6491	6452	6283	6282	6452	6490	6436	6286	6021	5950	5987	6002	5429	4604	
J	3868	4821	5601	5777	5967	5930	6010	6298	6471	6551	6554	6473	6473	6553	6550	6470	6296	6008	5928	5965	5774	5598	4818	3865
K	4055	5011	5530	5803	5988	5952	6037	6332	6514	6606	6627	6572	6572	6626	6605	6513	6330	6035	5950	5986	5600	5526	5007	4050
L	4234	5150	5608	5860	6046	6017	6101	6389	6562	6646	6659	6594	6594	6658	6645	6560	6387	6099	6014	6043	5856	5604	5145	4229
M	4322	5218	5659	5908	6112	6111	6192	6446	6589	6648	6629	6512	6511	6629	6647	6587	6443	6190	6108	6108	5904	5654	5212	4316
N	4322	5220	5670	5936	6177	6264	6340	6501	6600	6628	6574	6389	6389	6573	6627	6598	6498	6337	6261	6173	5931	5664	5214	4315
O	4231	5153	5630	5922	6188	6305	6378	6507	6581	6594	6525	6326	6325	6525	6592	6579	6504	6375	6301	6184	5916	5624	5147	4224
P	4045	5003	5540	5856	6129	6245	6316	6441	6515	6531	6477	6303	6303	6476	6529	6512	6439	6313	6241	6124	5851	5534	4997	4039
Q	3867	4789	5570	5774	6024	6110	6177	6325	6418	6455	6438	6353	6353	6437	6453	6416	6321	6174	6106	6019	5769	5564	4783	3862
R		4511	5319	5884	5896	5899	5960	6171	6295	6354	6362	6304	6304	6360	6353	6292	6168	5956	5895	5891	5878	5313	4506	
S		4034	4934	5627	5965	5716	5764	6004	6146	6220	6237	6187	6106	6236	6218	6144	6000	5760	5711	5960	5622	4929	4029	
T		3455	4350	5134	5621	5740	5599	5820	5958	6031	6037	5955	5955	6034	6028	5955	5817	5594	5735	5615	5129	4346	3451	
U			3778	4516	5129	5429	5664	5618	5746	5818	5809	5667	5666	5807	5815	5743	5614	5659	5424	5124	4511	3774		
V				3845	4437	4949	5322	5371	5538	5637	5639	5491	5490	5636	5634	5534	5366	5317	4944	4433	3840			
W					3671	4176	4670	5052	5314	5472	5514	5397	5395	5510	5467	5309	5047	4665	4172	3367				
X						3292	3789	4190	4511	4720	4814	4798	4796	4808	4713	4505	4185	3785	3288					
Y								3193	3470	3708	3831	3846	3841	3821	3695	3463	3187							

Power Groupings

7500	6400	
6400	6300	
6300	6000	
6000	5700	
5700	5400	
5400	5000	
5000	4000	
4000	3000	

Figure 5: Channel Power ranges and feeders affect subsequent behaviour

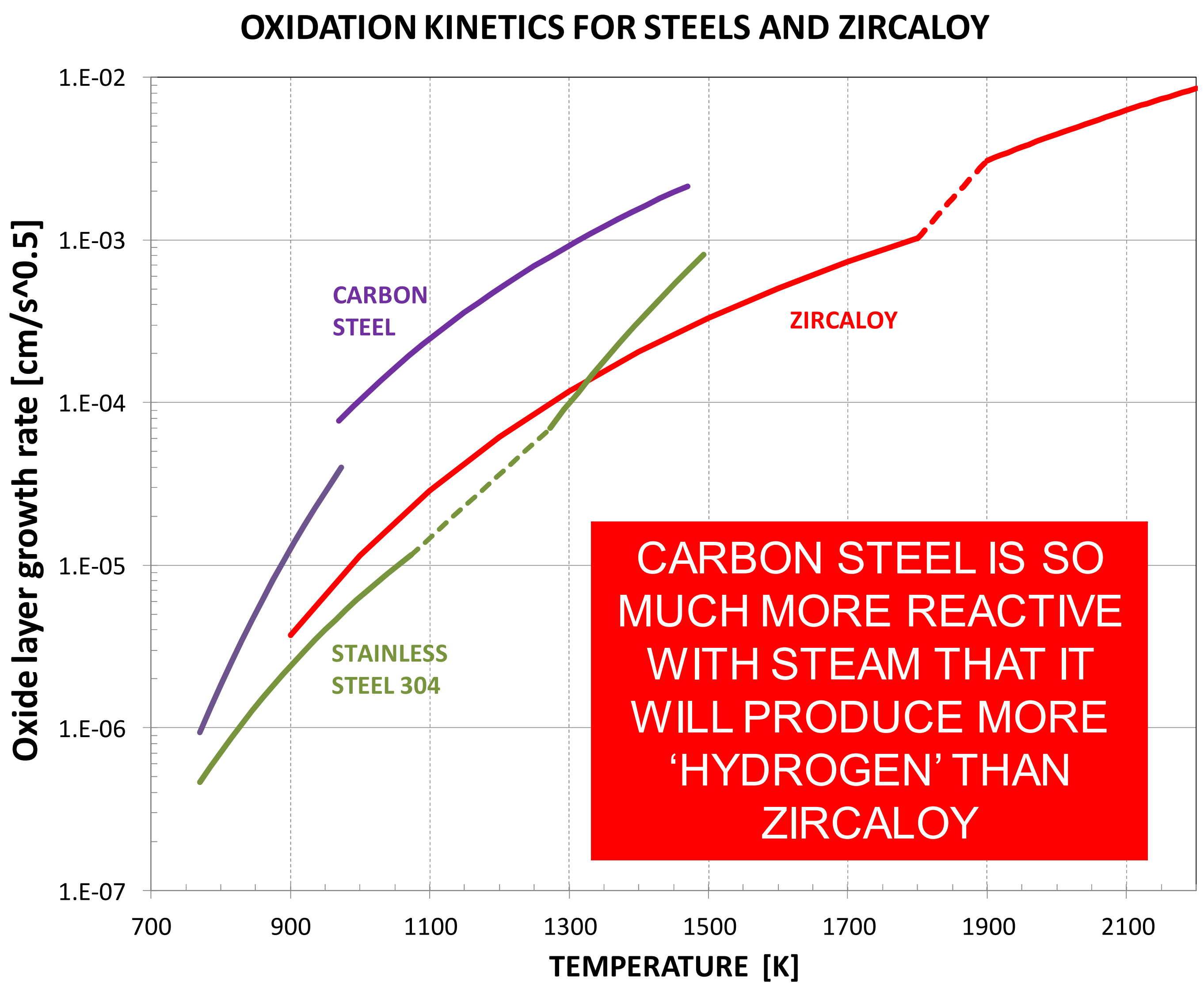
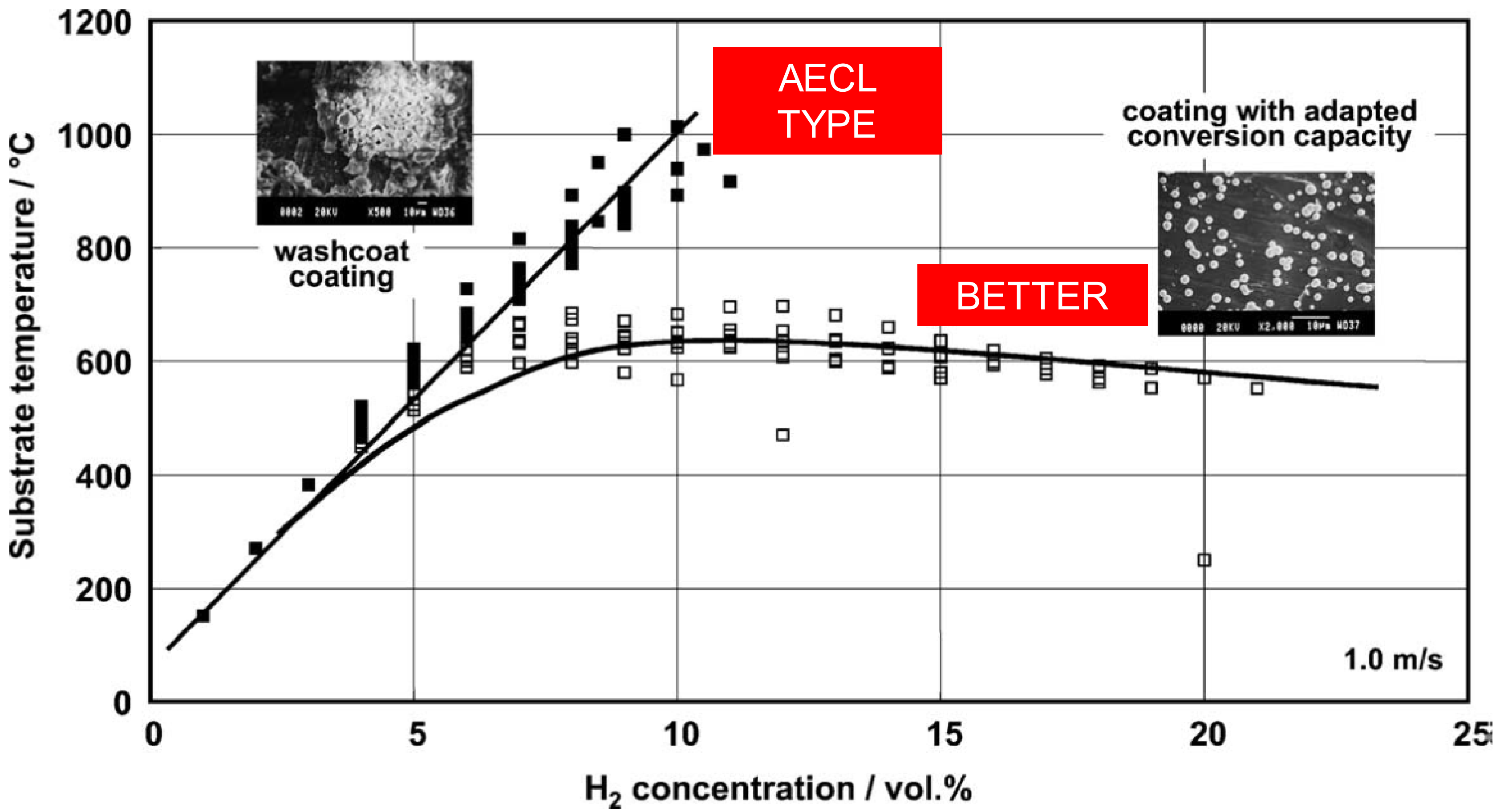


Figure 6 : Oxidation kinetics of different core materials



E.-A. Reinecke et al. / Nuclear Engineering and Design 230 (2004) 49–59

Figure 7: Typical PARS exit temperatures

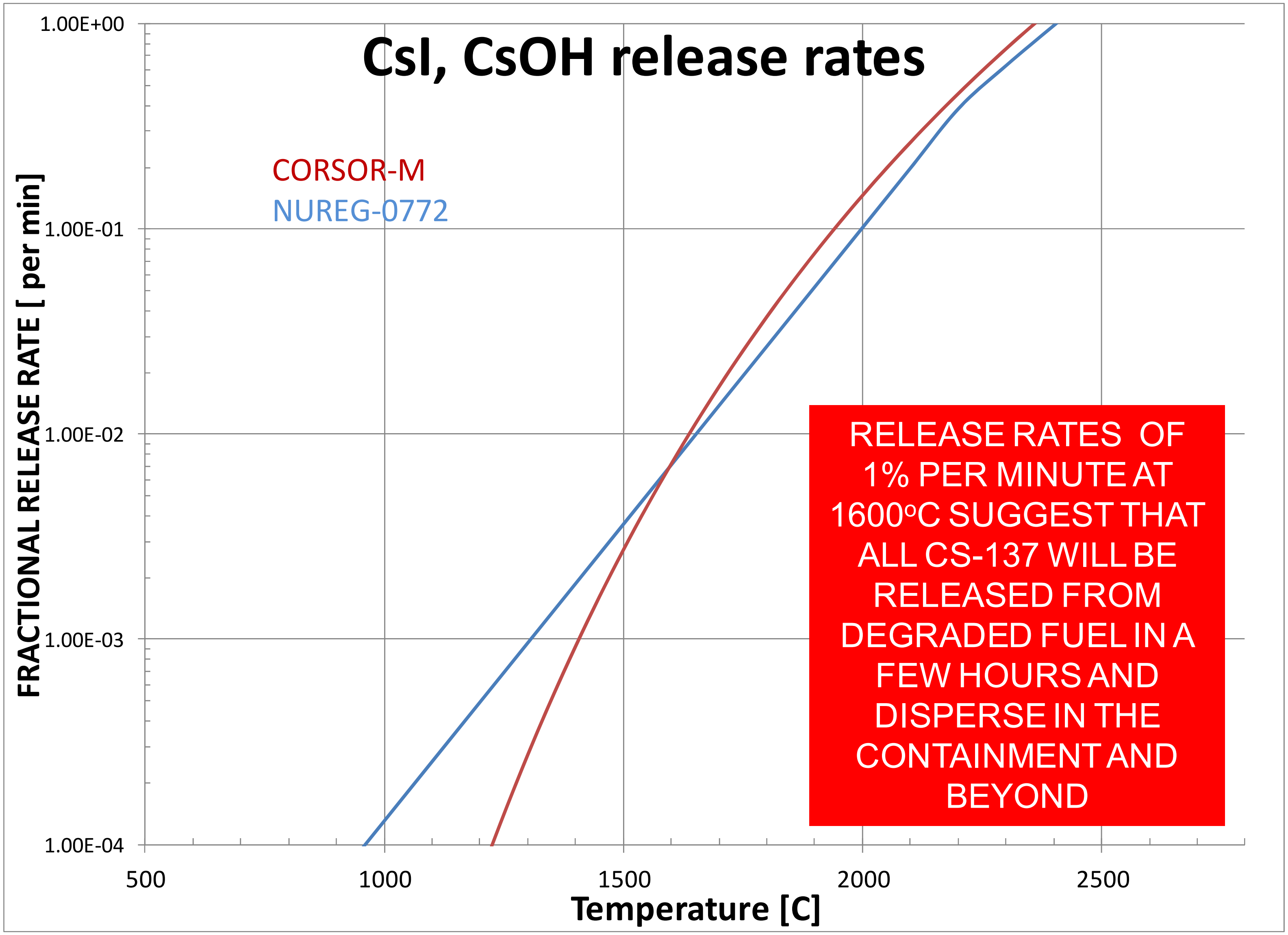


Figure 8: example of fission product release rates

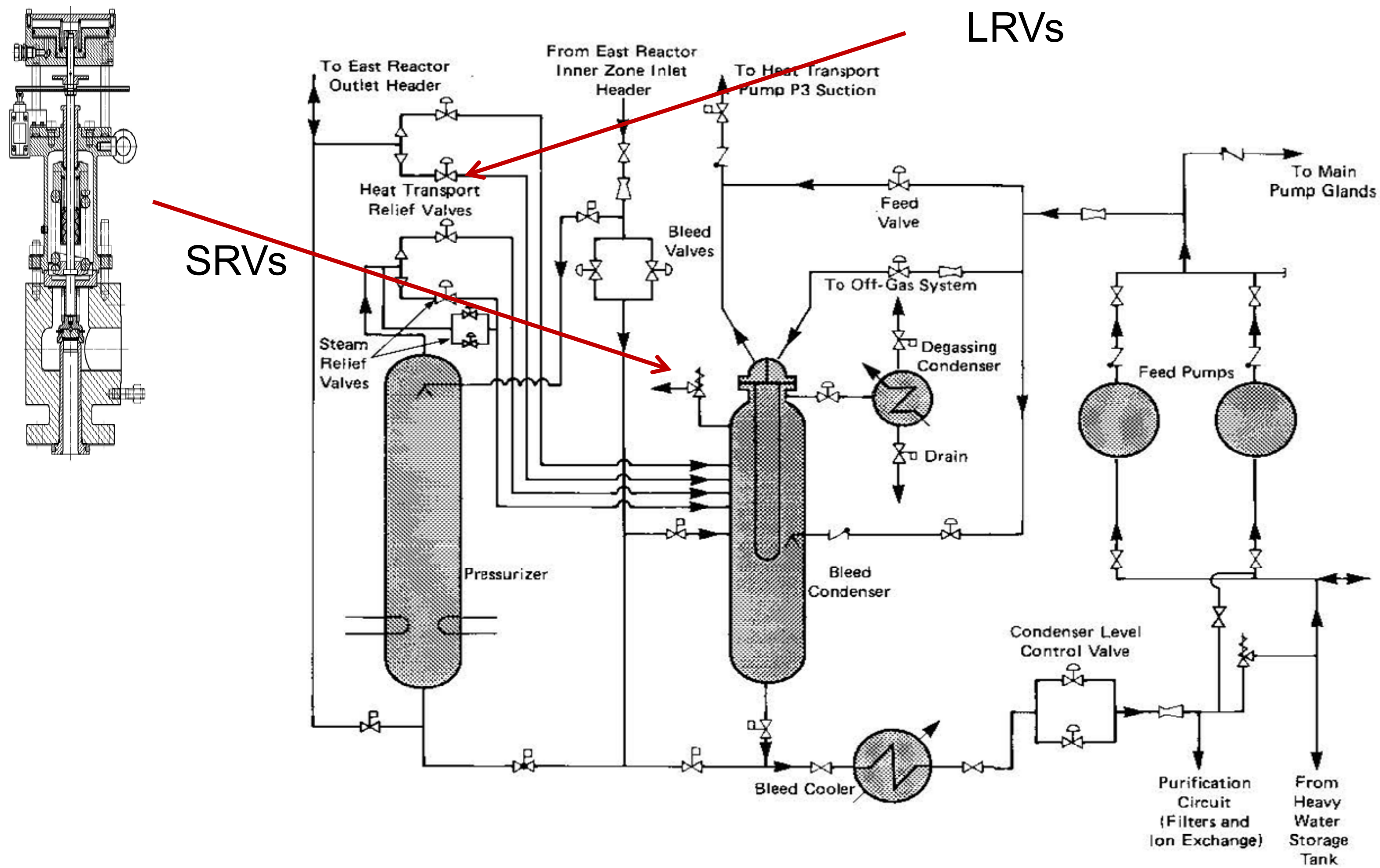


Figure 9: BRUCE CANDU HTS over pressure protection - Left arrow shows SRVS, right arrow shows LRVs

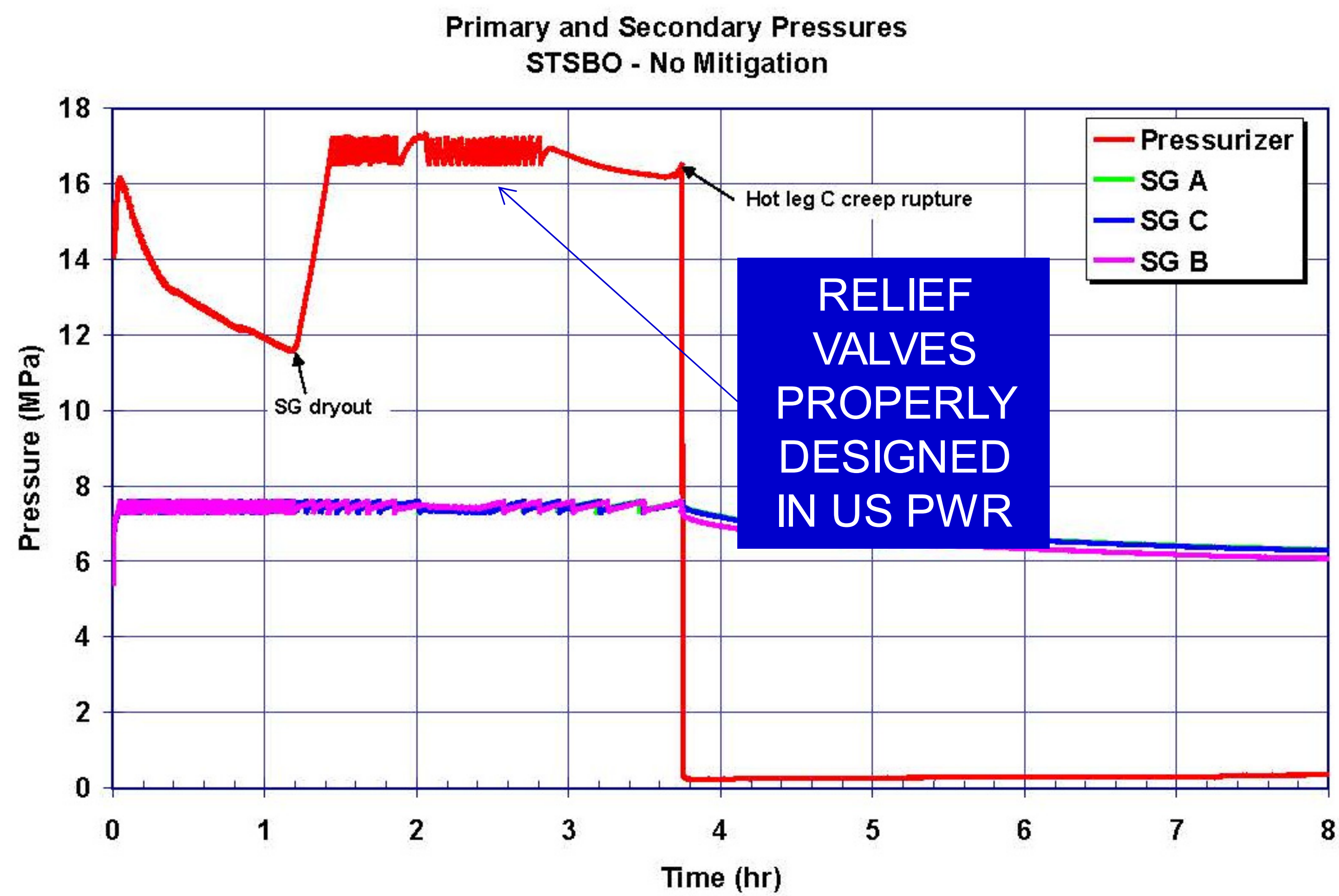
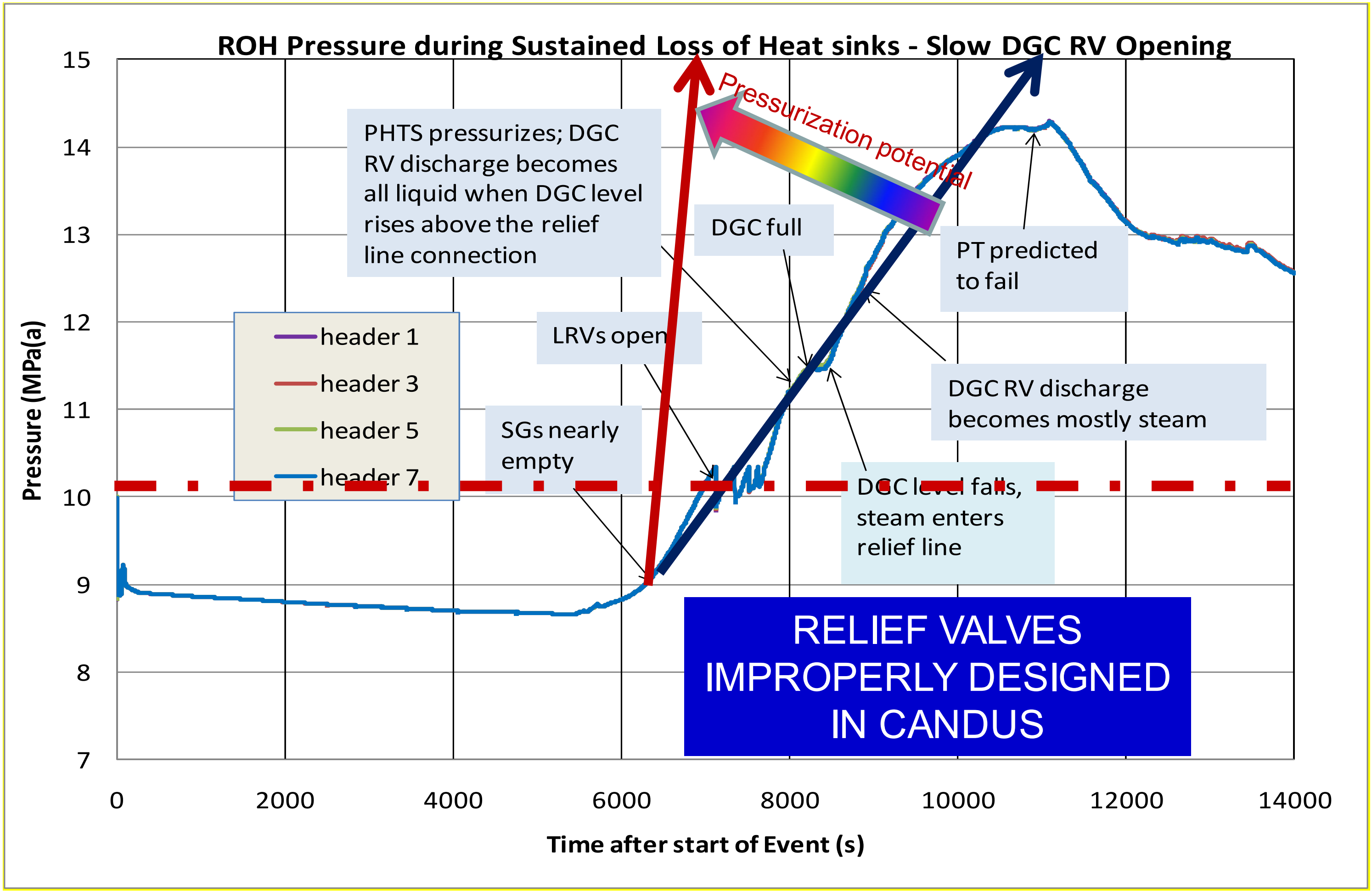


Figure 5-28 Unmitigated STSBO primary and secondary pressures history

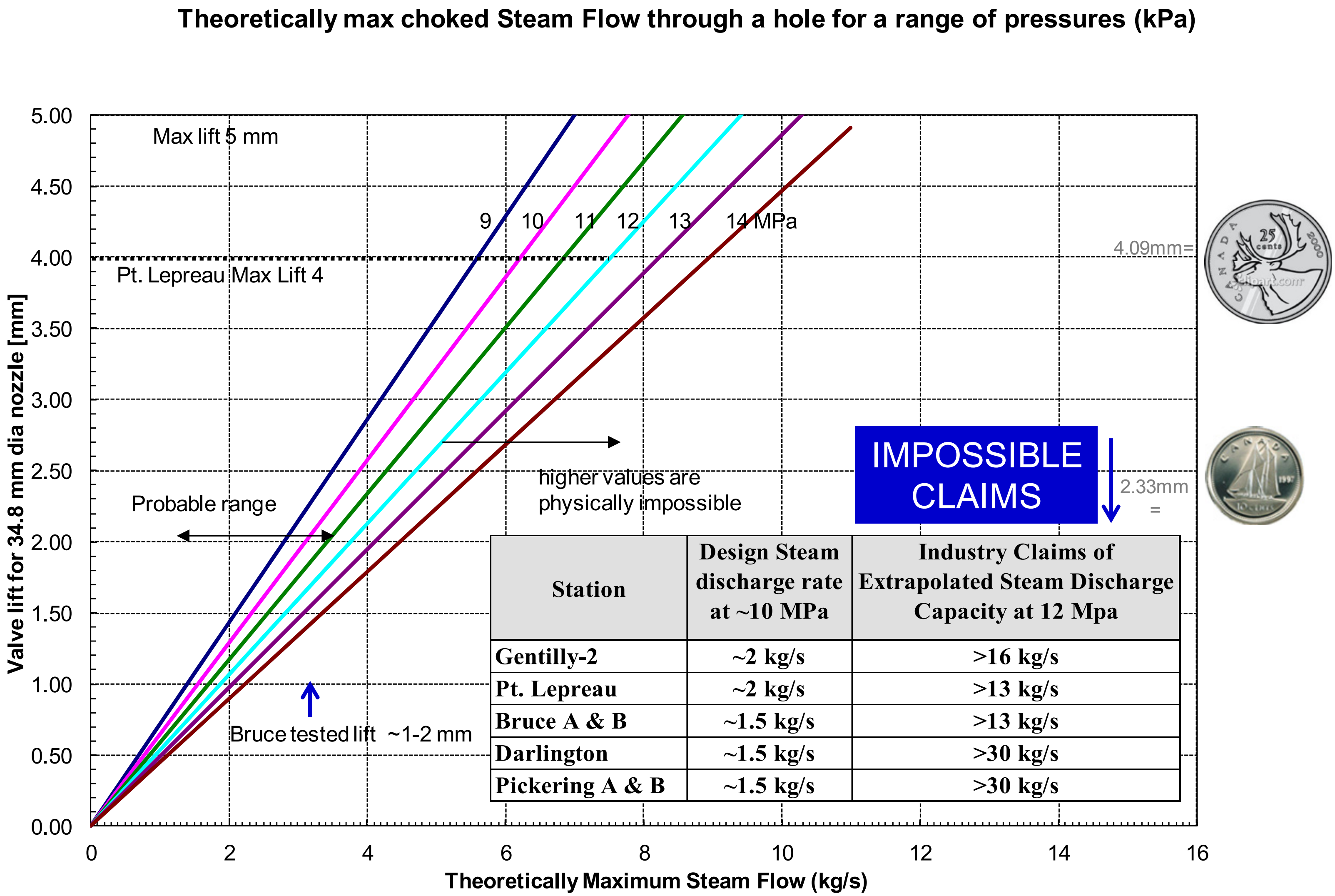
Source – NUREG/CR 7110

Figure 10 : Example of PHTS response to a properly designed relief valve



Source : AECL 2011

Figure 11 : A typical CANDU response to a loss of heat sinks - uncontrolled over pressurization due to improperly designed valves with inadequate steam relief capacity (AECL calculations with my arrows, dark blue notation)



Station	Design Steam discharge rate at ~10 MPa	Industry Claims of Extrapolated Steam Discharge Capacity at 12 Mpa
Gentilly-2	~2 kg/s	>16 kg/s
Pt. Lepreau	~2 kg/s	>13 kg/s
Bruce A & B	~1.5 kg/s	>13 kg/s
Darlington	~1.5 kg/s	>30 kg/s
Pickering A & B	~1.5 kg/s	>30 kg/s

Figure 12: Sample calculations to demonstrate that Bruce safety relief valves with 1mm lift cannot relieve enough decay heat steam (~20 kg/s) to avoid an uncontrolled rupture

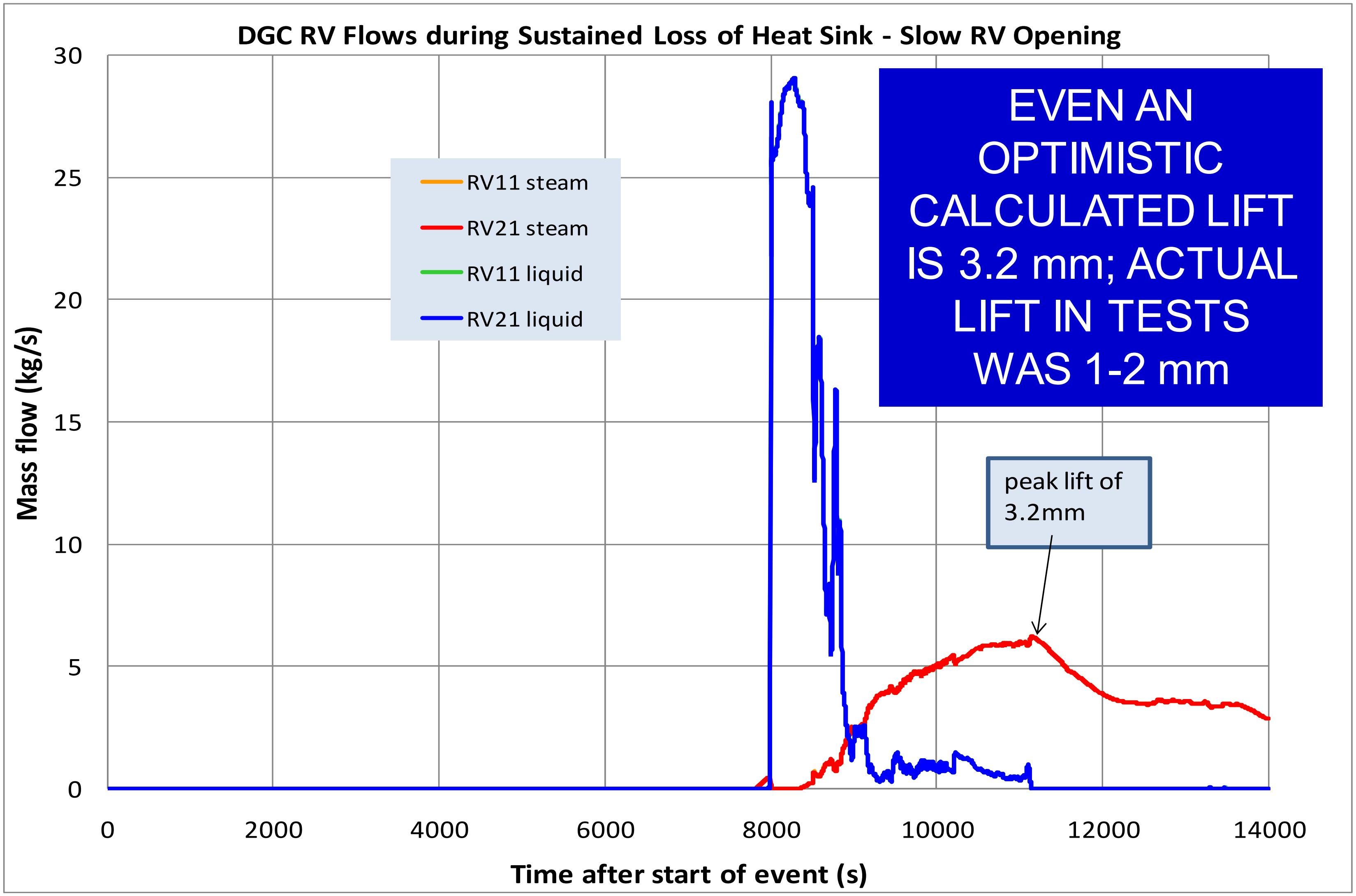


Figure 13 : AECL calculations confirming that the steam relief capacity of the Bruce type safety relief valves at <10 kg/s is inadequate and will cause uncontrolled ruptures

REFERENCES

1 The official report of the Fukushima Nuclear Accident Independent Investigation Commission, The National Diet of Japan, 2012.
2 Causes of and Lessons from Fukushima Accident, Won-Pil Baek, VP Nuclear Safety Research, KAERI, NUSSA 2012
3 CNSC Integrated Action Plan On the Lessons Learned From the Fukushima Daiichi Nuclear Accident, August 2013
4 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.

ATTACHMENT 2

N11P0543

Conversations about Challenges in Multi-Unit CANDU Reactor Severe Accident Mitigation Strategies

Sunil Nijhawan
Prolet Inc.
Toronto, Ontario M2K 1N4, Canada

ABSTRACT

Post Fukushima rhetoric of Robust Designs and Excellence in Regulatory Governance notwithstanding, containment design specific features of multi-unit CANDU PHWRs, that singularly house all four reactor cores within a single reactor containment volume, further exasperate the vulnerabilities of single unit PHWRs to accident initiators that can lead to severe core damage. There exist severe challenges to successful and positive outcomes from available accident management opportunities and potential for significant off-site releases is enhanced by the design decisions made over 40 years ago when severe accidents were unknown. Even without consideration of ageing effects, their small containments, with a design pressure of less than 100 kPa(g) and a design leakage at that pressure of up to 48% per day are likely to fail early and leak copiously under severe accident loads. They will also likely trap and hold within the reactor buildings, high concentrations of the combustible Deuterium gas and fission products ejected directly and un-attenuated from the degrading multiple reactor cores perched like inverted cups above an underlying common fuelling duct. Critical reactor components such as pumps, boilers, and reactivity control devices located outside the containment are extra vulnerable to external events. Contrary to design practices in all other PWRs that assure submergence of the reactor core with a pressurizer water level above the boiler tubes, the pressurizer in multi-unit CANDUs has been placed well below pumps at an elevation starting at about the bottom of the core. This has a number of unforeseen implications under severe accident conditions. A sustained loss of power will cause the pressurizer steam space to shrink and the low lying pressurizer vessel to gradually swallow some of the primary coolant liquid inventory. Decrease in loop coolant inventory will cause an early termination of thermosyphoning flows and hence of assured heat removal from the core, leading to cyclic over-pressurization and fuel heatup; turning an avoidable severe core damage outcome into a likely inevitable one.

KEYWORDS

CANDU Severe Accidents, Regulatory Actions, Fukushima Lessons, Darlington, Bruce

1. INTRODUCTION

The nuclear stations at Bruce, Pickering, and Darlington are home to 18 of the 19 operable CANDU reactors in Canada. The reactor cores are housed in multi-unit complexes of four or eight interconnected reactor buildings linked to a common 'vacuum building' (Figure 1). The reactor buildings are not designed or built like classical pre-stressed concrete cylindrical structures with hemi-spherical domes; they are composed of rectangular concrete slabs (like in industrial buildings) and have a very low pressure retention capacity (< 1 bar) and an extraordinarily high leakage by design.

For discussion purposes, this paper concentrates on severe accident related reactor design issues that are common to the relatively newer Bruce and Darlington reactors in Ontario, Canada. These reactors will see another 25 years of operation after their recent or now planned refurbishments. The units at Pickering, located at the edge of Toronto, the largest metropolitan city of Canada, are a decade older. Although another life extension is planned by the province for these reactors from mid 1960s, if the regulators do their job, the operational 6 of the 8 Pickering reactors should be on way to permanent shutdown soon. These units have significantly different and more importunate issues.

The multi-unit reactors at Bruce and Darlington were constructed between 1971 and 1993; and like all reactors of that vintage, did not consider severe accidents in the original design. Thus, they are not unique in requiring serious retrofits in this post Fukushima environment of public expectations of reasonable risk. They are unique, however, in having a utility and a compliant regulator deny any such need for design upgrades, and publish irresponsible and technically illogical 'studies' on the infallibility of the reactor design. Some measures to acquire additional backup generators and installation of filtered containment venting systems have been undertaken after Fukushima and will help marginally in risk reduction, while other retrofit measures such as passive autocatalytic recombiners (PARS) for 'hydrogen' mitigation have been undertaken without sound engineering analyses and can actually lead to an increase in risk (see sections 3.6, 3.7). However, recognition of a number of critical vulnerabilities by the utility and regulator alliance is still pending. A public conversation on these issues is the objective of this paper.

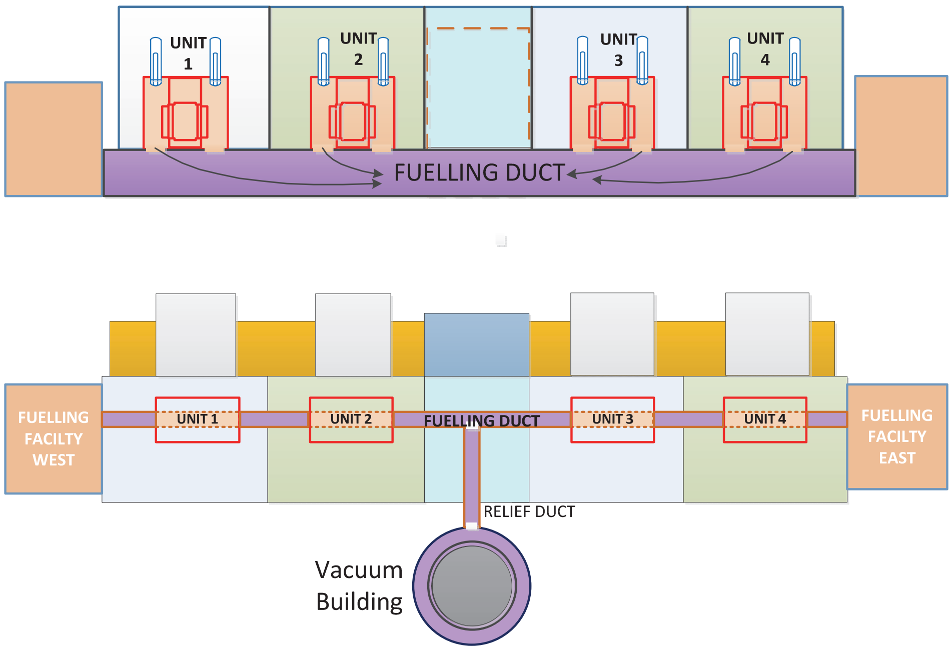


Figure 1: Typical layout of four reactor units at Bruce and Darlington

Most of the severe accident related vulnerabilities in the multi-unit plants, arising from the inherent 40 odd year old PHWR design, are common with those in the single unit plants (reference1). This should be of public concern since a multi-unit severe core damage accident will likely have significantly larger and unacceptable off-site consequences. However, the weak multi-unit containments and placement of critical components within them (such as the pressurizer below the core and boilers outside the containment), add additional vulnerabilities, which as illustrated below, create additional challenges to management of severe accidents for these 40 year old designs.

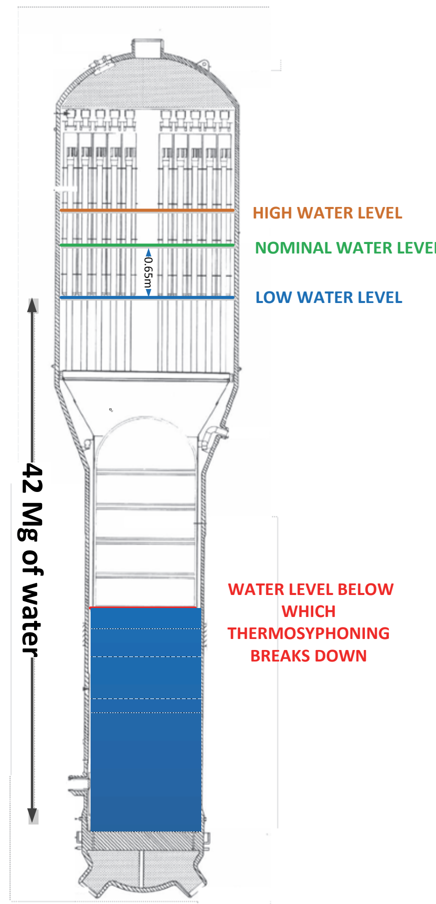
2. GENERIC CANDU ISSUES IN CANDU REACTOR RESPONSE TO A STATION BLACKOUT

All nuclear reactors must demonstrate an ability to withstand a loss of all normally connected AC power, including the Emergency Power Supplies, for a specified period of time. This is referred in the US to as The Blackout Rule - 10 CFR 50.63 which requires that core cooling and containment integrity be maintained for a specified station blackout (SBO) duration (defined using various design specific criteria, but typically two to sixteen hours) during which the onsite emergency power is also unavailable. US NRC Regulatory Guide 1.155 prescribes a series of design verification procedures for showing compliance with the SBO rule requirements. Standard review plan (SRP) addresses SBO with specific compliance verification directives. No such reviews or directives exist for Canadian PHWRs. The regulators have largely paid a scant lip service to concerns arising out of Fukushima reviews and the regulatory documents are largely without teeth.

It will be apparent from the following discussion of a select few number of design features discussed in reference to a station blackout scenario that a severe core damage accident at any multi-unit station has the potential of significant off site consequences and that accident management in absence of serious design upgrades will be marginally successful at best.

2.1 Significantly Short Steam Generator Heat Sink Effectiveness after a Station Blackout than Claimed

It is generally accepted that in absence of forced circulation of coolant by AC powered pumps, natural circulation of primary coolant is assured (for days) as long as the secondary side of the boilers and the primary side of core circuit are full of water and core decay heat is adequate. The secondary side water will boil away slowly as it removes the core heat. The current severe accident management guidelines require that in absence of restoration of power almost immediately, the steam generators must be manually depressurized for emergency low pressure water addition. It is not well understood that this must happen within approximately 45 minutes to an hour for Darlington reactor. The lower bound of the time estimate corresponds to pre-accident operation at boiler water level just above the low level trip set-point. We calculate that the initial inventory of about 42 Mg of water at Darlington becomes depleted enough in 45 minutes to cause the heat sink to become ineffective (boiler tube partial uncovery) and thermosyphoning flow, that maintains fuel cooling, to break down.



A 50-60% voided boiler secondary side may already be unable to promote thermosyphoning and at that time boilers become ineffective as a heat sink. The present severe accident management guidelines are based on an erroneous assumption that actual water inventory is about two times higher (82 Mg) and that 100% boiler inventory is available for heat removal. The utilities and the regulator CNSC staff continue to erroneously claim (reference 2) that not only would the boilers last for an incredible five hours but also that the deaerator inventory can magically flow into the pressurized boilers by gravity without operator intervention (reference 3).

Boiler water inventory in Darlington at low level trip level is 42 Mg. Difference between the low boiler level trip setpoint and the nominal boiler level is only 65cm. So the water inventory at the highest operating water levels cannot be much more than 45-50 Mg and last not much more than an hour before thermosyphoning flows breakdown as about 50% of the boiler tube surfaces get uncovered. The MAAP-CANDU analysis (code used by the multi-unit utilities) erroneously considers the boilers to be effective heat sinks until they are TOTALLY dried out (100% voided) and a number of additional mechanisms (such as a loss through check valves and initial fuel enthalpy) for boiler water depletion are ignored. The error in claiming that boilers are effective heat sinks for any more than an hour will have disastrous effect on accident outcome by misleading the planners of accident management emergency measures.

2.2 No Provisions for High Pressure Injection of Makeup Cooling Water to Steam Generators

There are no passive steam driven auxiliary feedwater pumps at multi unit CANDU plants (the single unit plant at Pt. Lepreau has one and many other PWRs around the world do too) or a method to easily replenish the voided steam generators with a high pressure emergency water injection. Under current plans, the omnipresent operator must manually depressurize the steam generators, which not only results in a loss of at least 40% of the remaining boiler inventory by flashing, but also creates increased potential for boiler tube failures (due to a two fold increase in pressure differential across ~15000 vulnerable boiler tubes) causing an undesirable direct, un-attenuated release of radioactivity into atmosphere by containment bypass. A high pressure (~5 MPa) emergency water injection into the boilers would have provided an intelligent accident management pathway and the obsession with boiler depressurization as the primary accident management strategy is wrong. The current Steam Generator Emergency Water addition system (water tanks on top of the building) can be easily upgraded to inject high pressure water into the boilers but is currently limited to a gravity feed.

The manual depressurization process can also waste over 40 precious minutes if the recommended cool down rate of 2.5^{o}C/min is followed. The depressurization process would cause a loss by flashing of about 40% of the precious steam generator fluid inventory. An effective accident management by manual depressurization requires not only that it be initiated in a timely manner, but also that the boilers be replenished as effective heat sinks well before the PHTS re-pressurizes to lose inventory through relief valves. No significant period during which the core heat removal by thermosyphoning through the boilers is interrupted can be tolerated. Once the primary system has re-pressurized and part of its inventory lost by relief (or drained into the pressurizer, as discussed below), no amount of addition of coolant to the steam generators, depressurized or not, will restore core cooling as a partially voided primary system cannot thermosyphon, especially with a loss of pressure control. The current primary accident management strategy for multi-unit plants is poorly rationalized and supported only by an arbitrary regulatory body claim of FIVE hours available to the operator to replenish the secondary side inventory (reference 2). Darlington analyses point to only 1 hour for operator action.

2.3 Low Lying Pressurizer Likely to Swallow Primary Coolant and Prematurely Interrupt Thermosyphoning Flows

The Darlington/Bruce pressurizer is at the lowest elevation of all primary circuit piping and components. In Darlington (and in Bruce), the bottom of the pressurizer starts at the elevation at which the very lowest fuel channel is also located (Figure 3). In comparison, a typical PWR pressurizer (also CANDU 6) is positioned higher than the pump bowls and extends to a height well above the top of the boiler tubes. Such a placement conforms to a simple, universally practiced design philosophy of ensuring that as long as the pressurizer water level is reliably maintained within norms, submergence in primary coolant of the lower elevation heat transport system including the core and the boiler tubes can be assured. The unconventional low placement of the pressurizer at Darlington and Bruce reactors can cause a significantly un-favorable outcome upon a sustained loss of power and result in much earlier and unexpected core heatup and fission product releases into the atmosphere.

Upon a sustained and unmitigated loss of normally connected AC power, an early passive heat removal by natural circulation (thermosyphoning) flows from core to the steam generators is required to be a long term heat removal pathway. But it is jeopardized in the Darlington and Bruce plants by the unfortunately low positioning of the large pressurizer vessel that can slowly swallow a large volume of the heat transport coolant from within the boiler tubes due to depletion of pressurizer steam volume. As the liquid inventory of the core coolant is relocated into the pressurizer, water level in the boiler tubes falls. When the level is low enough, liquid carryover is interrupted and the core loses the heat sink. No other PWR is known to position the pressurizer at the same elevation as the core. With such large emphasis on keeping the boilers full, the operator would not know that the pressurizer has induced a breakdown of thermosyphoning. Accident management will become very difficult.

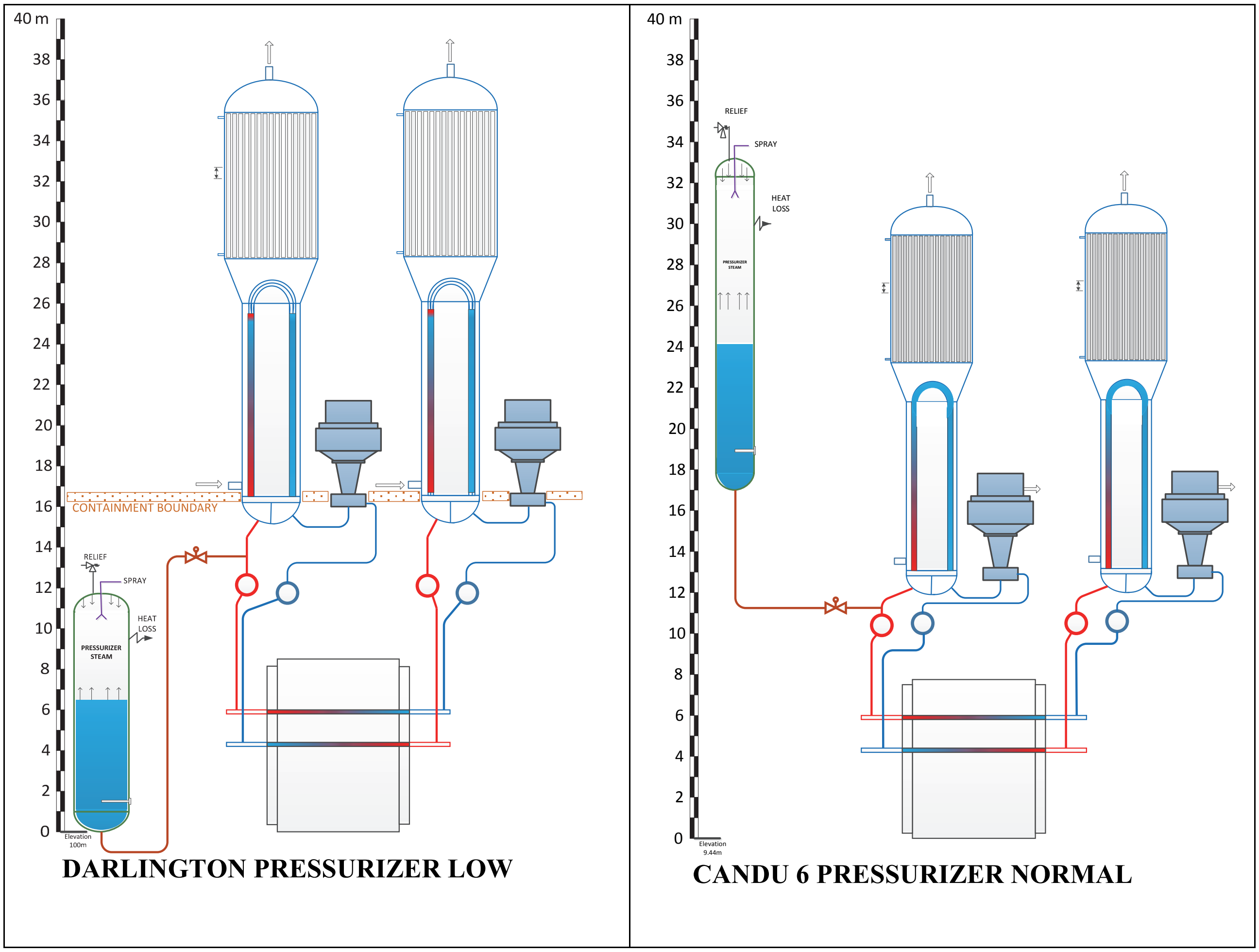


Figure 2 : Low placement of pressurizer makes draining of coolant from boilers and early termination of heat removal by thermosyphoning flows likely.

The expectation always is that the core cooling can be maintained for extended periods of time as long as water inventory on the secondary side of the boilers can be replenished. However, a slow collapse of isolated steam volume above the liquid level in the cooling pressurizer will start draining of the circuit inventory back into the pressurizer, terminating the thermosyphoning fluid carryover prematurely. Once the boiler tubes are partially voided and water level drops to a certain extent below the U tubes, thermosyphoning induced fluid carryover cannot occur OVER the U tubes.

Once all power has been lost the pressurizer steam space collapse can occur due to one or all of the following mechanisms:

1. Steam relief through pressurizer relief valves upon initial over pressurization within the first minute after reactor trip.
2. Steam relief through pressurizer relief valves upon a later re-pressurization.
3. Steam condensation on pressurizer metal walls due to heat loss.
4. Steam condensation on liquid interface due to liquid temperature drop as a result of heat loss from liquid part of pressurizer.
5. In leakage through liquid spray nozzle in the pressurizer steam space.
6. Out leakage of steam through valves and fittings and interfacing system piping.

2.4 Inadequacy of Overpressure Protection in Critical Systems

Under severe accident conditions when the boilers are no longer the heat sink, the heat transport system (HTS), the moderator and the shield tank assume the role of the dominant heat sink in succession and need to have a pressure relief capacity that can adequately remove steam equivalent of decay heat and any other loads that may be present. The reactor design, from 40 years ago when severe accidents were unknown, fails this basic design requirement that we now understand to be fundamental to accident mitigation and management.

None of the overpressure protection systems in the heat transport system, moderator or the shield tank are properly sized for severe accidents and cannot remove decay heat equivalent of steam when other means of heat removal are not available following an accident like SBO that may lead to severe core damage. An inability to discharge decay heat equivalent of steam from the primary cooling circuit around the core results in an over-pressurization and loss of circuit integrity. Initiation of boiling in the moderator (when the PHTS is voided and moderator is the dominant heat sink) leads to an unwarranted early partial ejection of moderator inventory and acceleration of core disassembly process. This is caused by inadequate steam relief capacity and activation of rupture disks. The inadequacy in shield tank relief capacity will cause that tank to rupture by over-pressurization after onset of boiling from thermal loads from debris contained within the Calandria vessel. While all three need to be corrected, of greater concern is the inadequate overpressure protection in the heat transport system.

2.5 Likely Uncontrolled Over-Pressurization and Rupture of Reactor Pressure Boundary upon Loss of Heat Sinks due to Inadequate Overpressure Protection

CANDU multi-unit reactor overpressure protection on the main HTS is atypical of pressurized water reactors. Instead of being a direct and unobstructed relief path as required by the ASME code, section III, NB-7141 (b) - it is composed of two sets of valves in series, separated by a small low pressure vessel called the bleed condenser or degasser condenser (Figure 3). The first set of valves are typically called liquid relief valves (LRVs) and the second set of valves are called safety relief valves (SRVs), although both sets are designed in CANDUs for a certain liquid relief. Specifications for both sets of valves are clearly for liquid relief only. The magnitude is typically based on a design basis scenario of D_2O bleed flow closed with D_2O feed flow full strength in. The SRVs have a very small steam relief capacity, not certified by tests for Darlington, and tested at Wylie Labs to be about 2 kg/s for Bruce. This tested relief is inadequate for the SRVs to remove decay heat (need a steam relief capacity of 30 kg/s to relieve 30 MW at 10 MPa).

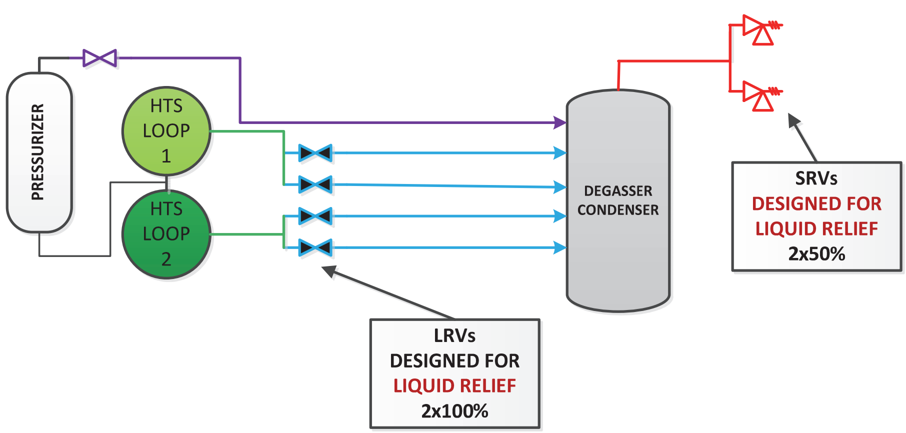


Figure 3: Overpressure protection system showing SRVs located downstream of other normally closed LRVs, both designed for liquid relief

When steam generators have failed to provide an adequate heat sink, these valves will maintain a constant heat transport pressure if they are able to pass enough steam (~30 kg/s) to match that produced by decay heat, in order to avoid an overpressure. So, upon loss of boilers as a heat sink, the system re-pressurizes and attempts at this time to avoid an overpressure by rejecting the decay heat through safety relief valves. An inadequate steam relief capacity (tests at Wylie Labs for Bruce safety relief valves confirm this) leads to a continued over-pressurization. Consequently, a loss of steam generator heat sinks leads to an unusual (for a nuclear power reactor) over-pressurization of the heat transport system, and an unavoidable, uncontrolled failure of a pressure boundary component. The failure is most likely to be in ever so vulnerable steam generator tubes, resulting in a potential containment bypass and early population exposure to fission and activation products. Analyses at AECL claimed a potential failure of a fuel channel instead of a number of steam generator tubes. There is ample data on steam generator tube failures to dispute that outcome. Any uncontrolled rupture due to over-pressurization at this stage is an unfortunate and undesirable outcome, contrary to the ASME requirements for pressure vessels.

2.6 Inability to Add Water to Heat Transport System at High Pressures

While high pressure water addition systems (e.g. feed system) exist as part of the pressure and inventory control systems under normal operation, there are no provisions to augment losses from the PHTS at high pressures using any emergency measures after a station blackout or a similar accident that results in a pressurized heat transport system imminently under threat of pressure boundary rupture.

With neither 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, an uncontrolled rupture becomes an unnecessary inevitability with a potential for an early containment bypass.

3. CONTAINMENT STRUCTURE VULNERABILITIES

In addition to the horizontal channel design of the PHWR cores, what distinguishes the Darlington and Bruce multi-unit plants from all other multi-unit stations around the world is that each plant uses a containment structure that is common and contiguous to four relatively large reactor power units, each about 2700 MW(th) - see Figure 1. As a result, any accident that results in activity releases into the containment, whether within the design basis or not, is likely to contaminate all reactor units.

A common fuelling machine duct underlying the four reactors connects the containment volume via a pressure relief duct to a vacuum building whose volume is about 75% of the volumes it is expected to depressurize following an accident. It is deemed adequate for design basis accidents in a single unit, but its effectiveness to mitigate an accident in all four units is lacking. The containment is built to the national building code as are the access requirements, fire protection, smoke detection, etc.

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 at Darlington; a combined volume of the four unit reactor buildings, 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 ~10 kPa(a) with the main containment volume slightly sub atmospheric at ~98 kPa(a). 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. Comparison of containment data from other reactor types is summarized in Table 1. Significantly high containment leakage rates at design pressure, small containment volume to thermal power ratio, and a low pressure retention capacity makes the multi unit CANDU plants in Canada highly vulnerable to causing excessive radioactivity releases upon a core damage accident.

Table 1: Comparison of CANDU containments with containments in operating US power plants

	BWR Containment Design/Types			PWR Containment Design/Types			CANDU Single Unit PHWR	CANDU Multi-Unit PHWR
	Mark I	Mark II	Mark III	Sub-atmospheric	Ice Condenser	Large-Dry	Cylindrical / dome	Industrial slab
Number of Units	24	8	4	7	9	57	6	5 * 4
Reactor thermal power (MWth)	1593 - 3293	3293 - 3323	2894 - 3833	2441 -3411	3411	1500 - 3800	2056	2776
Volume, (thousand m3)	12	15	48	52-70	36- 40	46-100	48	21
Containment design pressure (MPa)	0.49-0.53	0.41-0.48	0.2	0.41-0.52	0.18-0.31	0.38-0.52	0.124	0.05 - 0.09
Containment free volume (thousand m3)	15.86	25.63	49.43	54.93	36.62	79.34	48	21*4 +95
Cont. volume to thermal power ratio (m3/MW)	7.53-3.64	4.51-4.56	12.52-16.59	20.52-21.30	11.14	26.32 - 30.67	23.35	16.12
Median containment failure press (MPa) in IPE	0.78 - 1.41	1.07- 1.42	0.49-0.75	0.93-1.00	0.35-0.76	0.72-1.41		
Containment construction	22 steel	1 steel	2 steel	7 concrete	7 steel	7 steel	concrete	concrete
	2 concrete	7 concrete	2 concrete	-	2 concrete	50 concrete		
Allowable Leak Rate (volume %/day)	0.5	0.5	0.4	0.1	0.25	0.1	5	48
LWR data taken from ocw.mit.edu/courses/nuclear-engineering/22-34j-structural.../doro.pdf								

3.1 A Number of Critical Reactor Systems outside the Containment Boundary

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 (Figure 4). 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. There are no new improvements to pressure suppression systems in reactor buildings and as such, the vacuum buildings may be inadequate to avoid building failures. Measures to reinforce the confinement pressure boundary (space occupied by safety and process systems outside the containment) have not been undertaken.

3.2 Station Structures Well Below the Level of the Lake and Susceptible to Flooding as in Fukushima

The basement of the reactor buildings (fuelling machine duct and the pressure relief duct) are located below the level of the water in the lake (Figure 5). To the credit of the utilities, newly acquired emergency diesel generators have been located at elevations higher than the original emergency generators that are still at lower elevations.

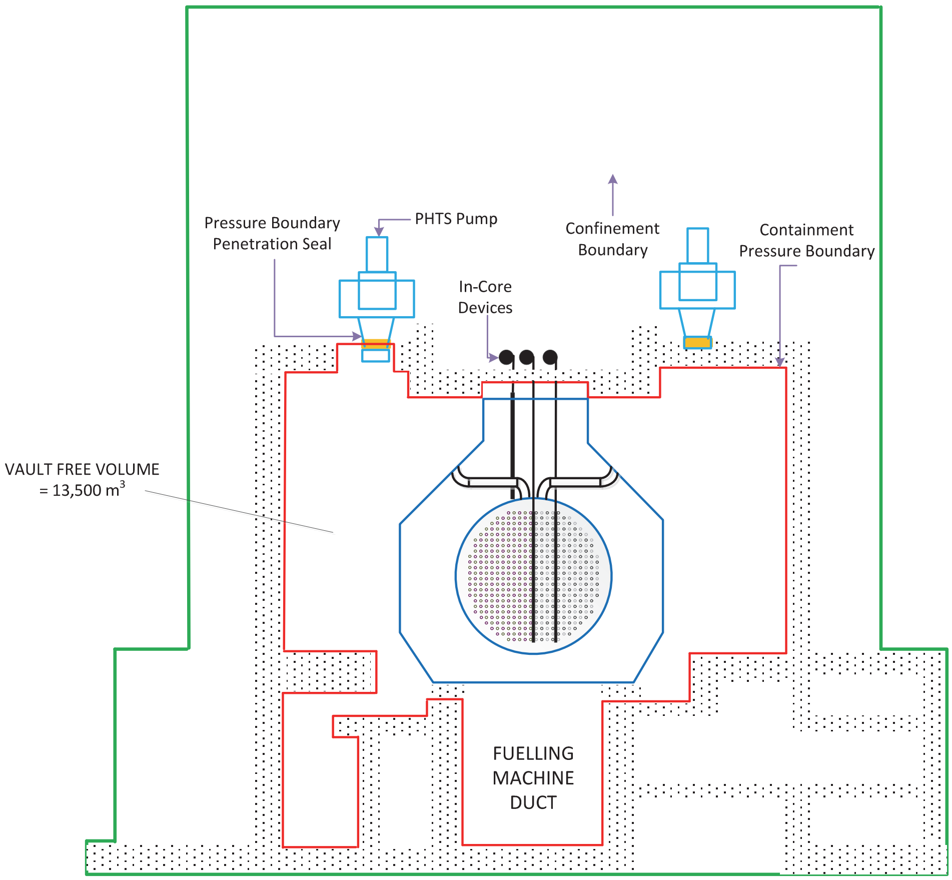


Figure 4: Reactor building cross-section for one of the four units showing a common fuelling machine duct. See also Figure 1. Boilers protruding out of the containment top boundary not shown.

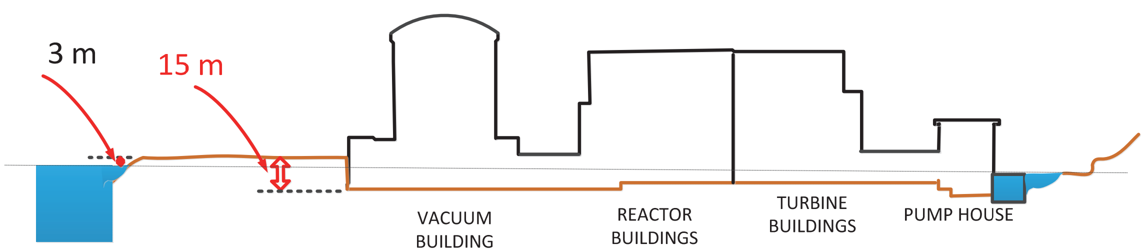


Figure 5: Building basement layout below Lake water level and susceptible to flooding.

3.3 Extremely High Design Leakage Rate from Containment Structures

The multi unit containment structures are composed essentially of rectangular concrete slabs which differ significantly from typical cylindrical PWR containments with hemi spherical tops and steel cable pre-stressed concrete. As a result they and have a relatively weak design pressure (0.6 to 0.9 bar compared to ~5 bar for PWR containments) with relatively high design leakage at design pressure (up to 2% volume per hour or upto 48% per day comparing very unfavorably to a typical US PWR with 0.1% leakage per day (Figure 6) at a design pressure that is typically five times higher for PWRs). As a result the Bruce/ Darlington containments can fail early and allow large releases of radio activity into the atmosphere once an accidental activity release occurs from the overheating fuel.

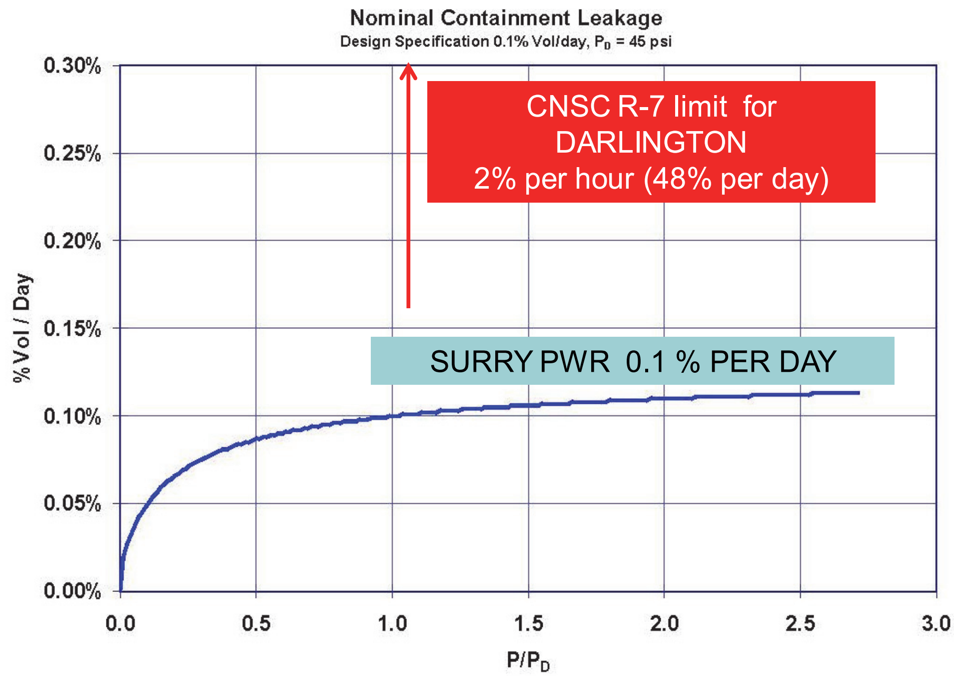


Figure 6: Comparison of a PWR containment design pressure leakage with that for a multi-unit CANDU (note that the Darlington leakage rate is way off scale and abnormal for a nuclear reactor).

3.4 Even the Low Containment Pressure Retention Capacity Not Tested for Many Years

The multi unit CANDU containments are tested for pressure retention most infrequently of any power reactor in the world. Darlington now tests just the vacuum building (and not the containment around the reactors) for pressure every 12 years while the regulations (section 5.2.2 of reference 4) under which it was originally licensed required a six year test interval for both the containment as well as the vacuum building. The last vacuum building pressure test at Darlington was described as a 'difficult and arduous process' that took six months of planning. The Bruce vacuum building has not been tested for overpressure since 1992.

3.5 Containment Receives Fission Products and Deuterium Unmitigated and Largely Un-attenuated

A severe core damage in a CANDU reactor is typically caused by a loss of primary coolant coupled with a loss of moderator that surrounds the horizontal fuel channels as a heat sink of last resort. The reactor design is such that a severe core damage accident would, in absence of a pressure vessel to contain the debris, result in an unattenuated and direct discharge of energy, combustible gases and fission products into the inverted cup like reactor buildings that offer outlets for incoming gases only at the bottom (Figure 7). This is a result of a huge discharge path created by Calandria vessel rupture disks and an absence of an adequate controlled steam relief on that vessel.

Once the heat transport system is voided, the fuel bundles in fuel channels heatup to reject heat to the moderator. The moderator water becomes the heat sink. Once the moderator water boils and pressurizes the calandria vessel enough to rupture the rupture disks (at ~130 kPa(g)), all further discharges from the moderator are directed into the containment through large 16" discharge pipes. In absence of a retaining pressure vessel like in LWRs, a fuel channel heatup and disassembly upon loss of moderator coolant puts energy, radioactivity and combustible gases directly into the relatively weak reactor buildings. These 'containment' structures are quite different from a traditional PWR cylindrical dome building and are rectangular structures built to old industrial standards.

A typical fuel channel response during a severe core damage accident initiated by a sustained loss of AC power in a station blackout scenario shows (Figure 10) that the fuel temperatures can be in the 1300^{o}C range attesting to the prediction of large fraction of core fission product releases into the containment. In these temperature ranges, the rate of fission product releases can be as high as 0.1% to 1% per minute (Figure 9) as per release correlations in NUREG-0772. With fuel sheath failures occurring early at a temperature of ~800^o C, 100% of noble gases and large amounts of tritium will escape from each failing fuel channel bundle. With a large variation in channel powers and a gradual channel uncovery in depleting moderator water level, fission product releases into the containment from various channels occur over a large period of time. As a result, the relatively leaky containment hosts high levels of combustible gases and fission products. Note that the reactor vault geometry provides ample hydrogen traps & relatively poor chances of any mixing. Therefore hydrogen explosions are very likely. At a minimum the relatively leaky containment will cause continuous release, without any holdup period, of significant amounts of radioactivity into the atmosphere.

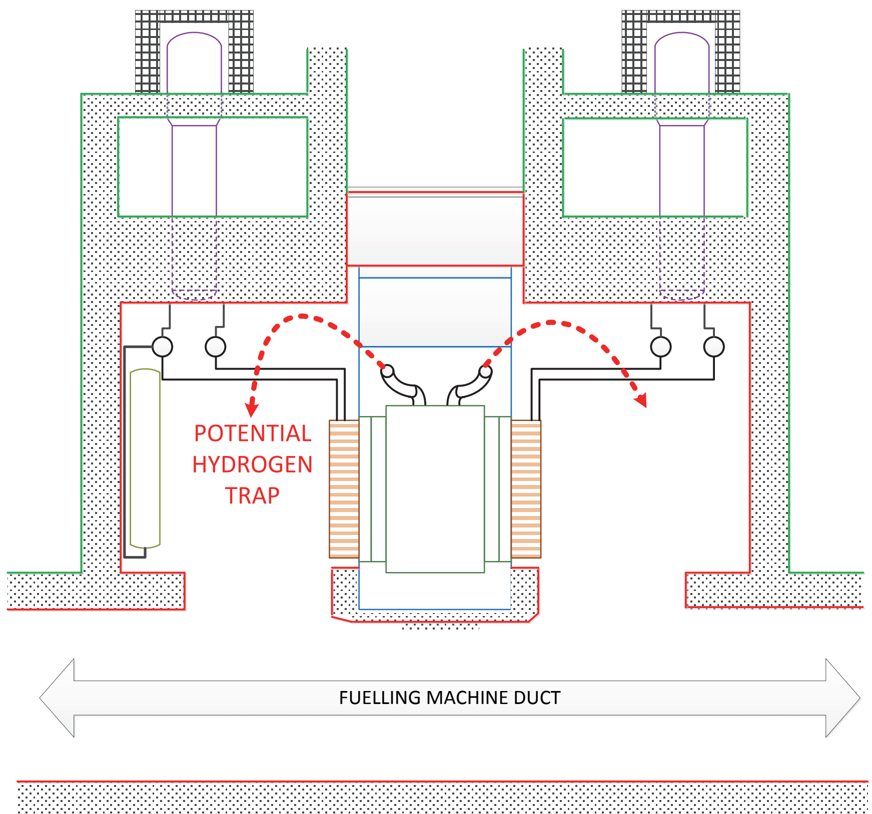


Figure 7: Direct expulsion of fission products into reactor building and entrapment of D_2 gas

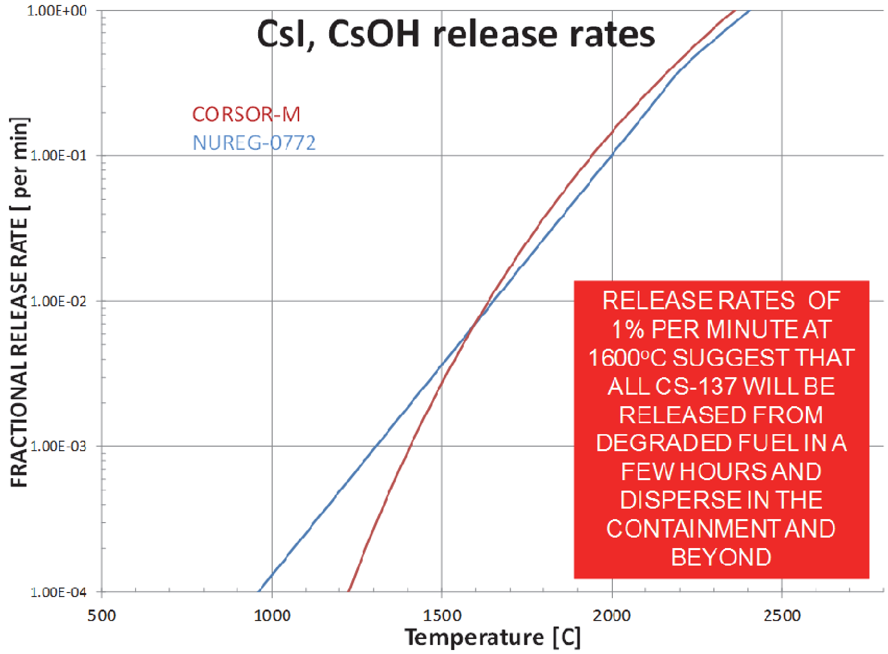


Figure 8: Cesium release rates from fuel as a function of temperature (sheath failures occur at around 800º C and all noble gases release at that point)

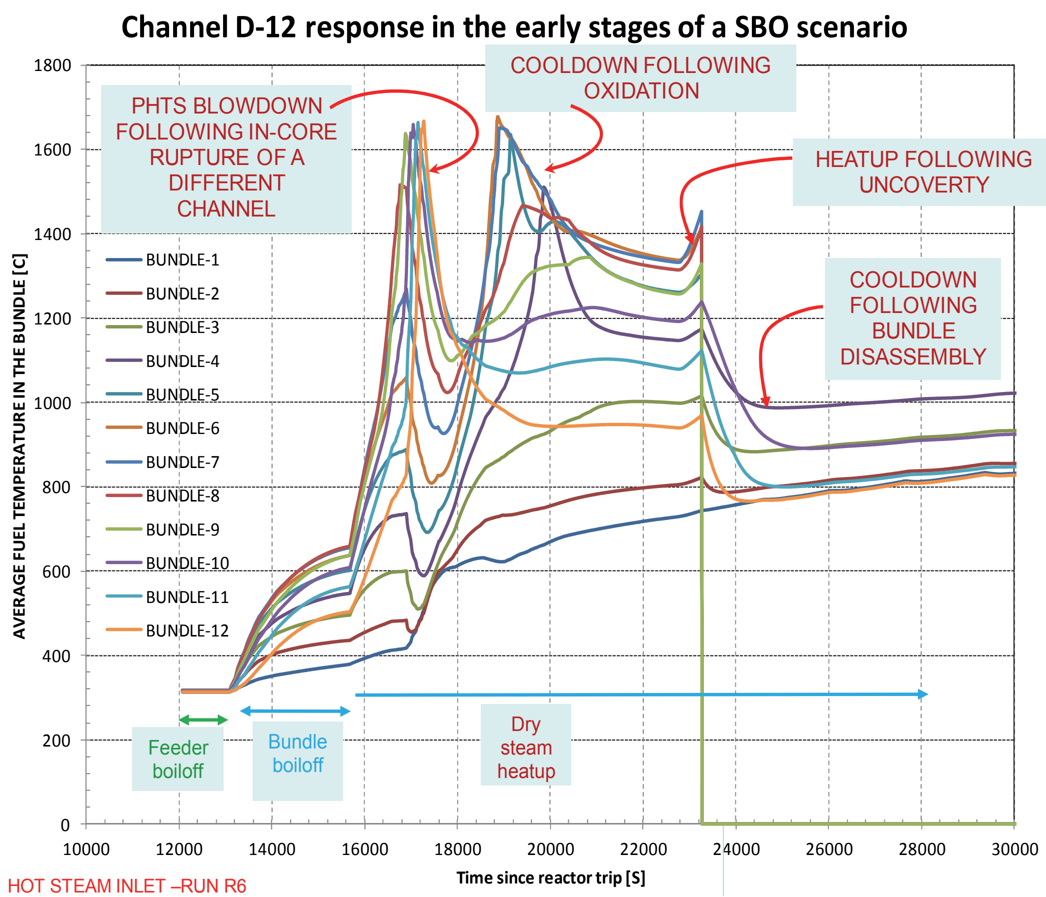


Figure 9: A typical channel thermal transient for 12 bundles in a CANDU six single unit reactor (using computer code ROSHNI, reference 5).

3.6 High Potential Combustible Gas Production

There are a number of issues regarding combustible gas (hydrogen) production in a multi-unit CANDU after a severe accident. Severe accidents in these reactors have a potential to produce large amounts of combustible gas due to copious amounts of Zircaloy and an abundance of exposure to large amounts of carbon steel in the reactor piping. However, the mitigation measures that have been proposed are for orders of magnitude lower combustible gas estimates. These were developed for design basis accidents (65 kg of H_2 in from fuel channels[1]) and are gross underestimates of the potential combustible gas source term from severe accidents (calculated independently to be in the range of 3000 kg of D_2). In addition, the 'hydrogen' mitigation systems - igniters and recombiners have been mistakenly designed for the wrong gas – Hydrogen (H_2) instead of Deuterium (D_2), which will likely be the only gas produced by the interaction of hot D_2O steam with metal. This mistake is unfathomable for a reactor system that uses D_2O and not H_2O s coolant and moderator.

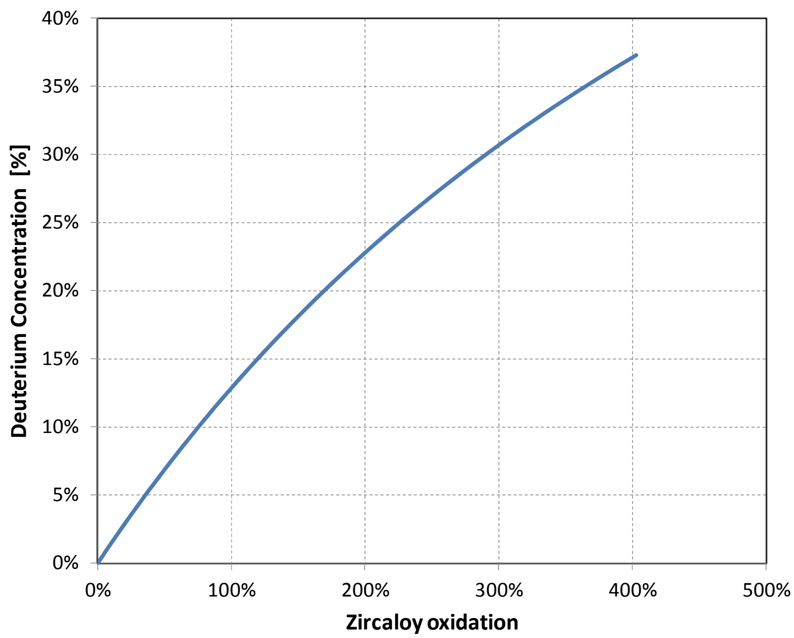


Figure 10: Average Deuterium concentration as a function of Zircaloy oxidation (100% from one unit, 400% from four units).

To make matters worse, the utilities and the regulators deny any difference between H_2 and D_2 and COG claims that the two gases are the same in combustion and recombination. They definitely are not. A large number of scientific papers attest to that (e.g. references 6, 7). Theoretical considerations suggest that Deuterium would recombine at least 41% slower and burn quite differently just from diffusion estimates. The two major sources of early (short term) combustible gas production that distinguish the multi-unit PHWRs from other reactors are obvious from examining the core layout. The core of each of the reactors contains about 60,000 kg of Zircaloy and the carbon steel piping offering over 2000 m^2 of surface area and over 120 tons of easily susceptible to steam and air oxidation carbon steel mass. Carbon steel in the 960 feeders (over 12,000 m in length) that connect each fuel channel at either end may contribute to more early D_2 production than Zircaloy in a severe accident scenario. Note from Figure 11 that carbon steel oxidation is faster than for Zircaloy at all temperatures. High rates of D_2 production will result in early concentration exceeding detonation

[1] This source term of 65 kg of H_2 was obtained without considering steel oxidation. Analysis now shows that carbon steel feeders produce enough flammable Deuterium gas for a sustained LOCA+LOECC scenario lasting many hours to make the Zircaloy source Deuterium look inconsequential.

limits. A containment average of Deuterium concentration as a function of Zircaloy oxidation alone is presented in Figure 10. Recall (Figure 7) also that the reactor buildings will trap gases which will make local concentrations even higher.

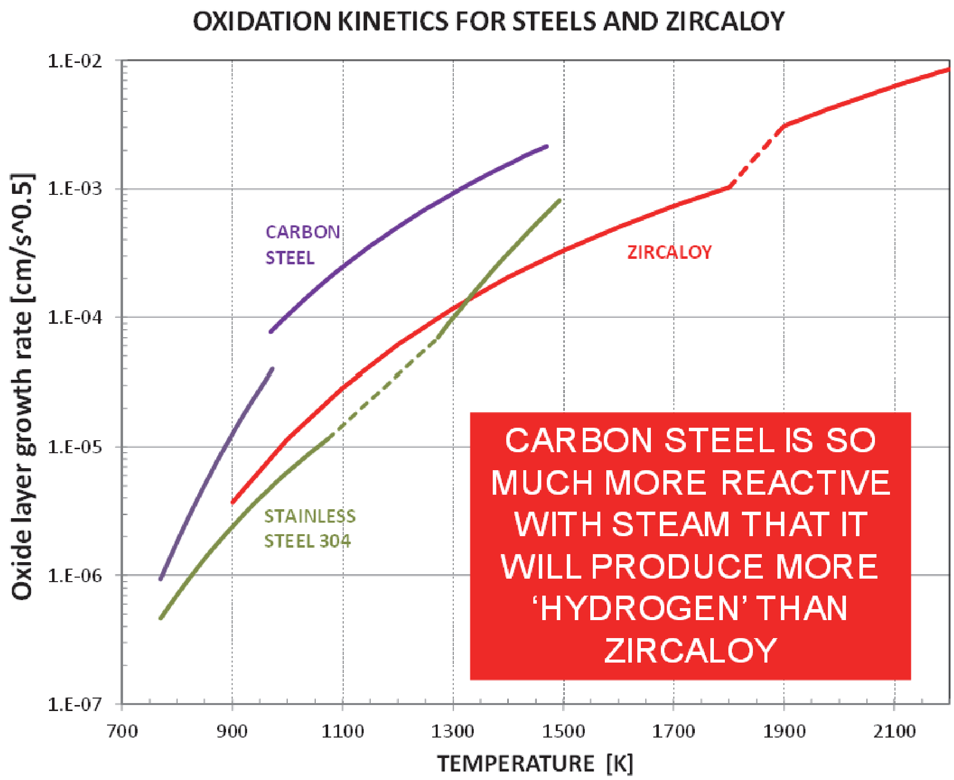


Figure 11: Relative oxidation rates for carbon steel, Zircaloy and stainless steel.

3.7 Passive Autocatalytic Recombiners (PARS) Poorly Designed and Engineered

Installation of PARS has become an acceptable hydrogen mitigation system for severe accidents because of their passive action, relatively well understood phenomenology, start-up at low hydrogen concentrations, efficiency under both beyond-design-basis and design-basis accident conditions, as well as implementation that does not constrain normal operation.

Yet, there are three issues that must be considered:

1. *The PARS units should be sufficient in number and placement to avoid a hydrogen burn (limit hydrogen concentration to less than ~4%). Tests have shown that at any concentration greater than 5%, these units with a wash coat layer of the catalyst exude flames. There are other designs of catalytic plates (*Figure 12*) that do not have this problem as by limiting the recombination rate the maximum substrate temperature is limited to below the auto-ignition temperature of hydrogen. At 6% hydrogen concentration the PARS units cause ignition leading to potential explosions. With such performance characteristics, installing no PARS at all is a better option than the small number of PARS currently installed if the hydrogen concentration cannot be guaranteed to be kept well below 4%.*
2. *The PARS units should be qualified (sized and tested) for the actual flammable gas (Deuterium in CANDUs) and not just for simple hydrogen. Data shows that processes that dominate recombination by a catalyst may be slower by a factor of up to √2 for Deuterium. None of the installed units were tested for Deuterium. They were tested for common, lighter Hydrogen. CANDU severe accidents result in production of Deuterium first and predominantly so.*

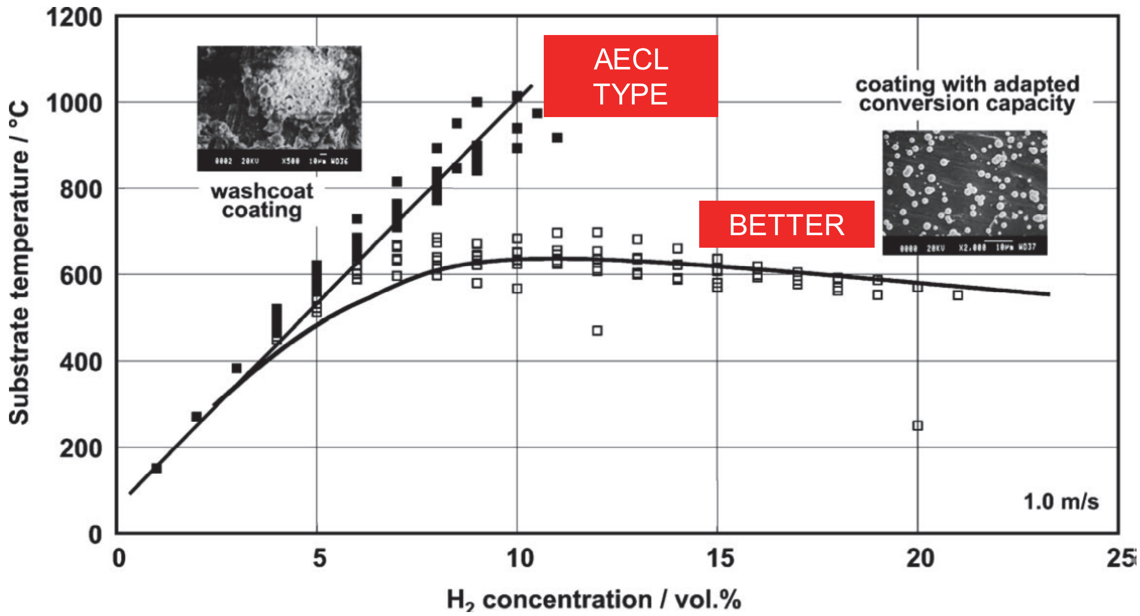


Figure 12: Recombiner temperatures that can cause explosive interactions at high local hydrogen concentrations (from reference 8, red tags added)

3. *PARS units should not cause a containment failure by the heat of recombination reaction or by the fires potentially caused by the high temperature gases exiting the PARS units. The recombination kinetics for hydrogen is:*

$$H_2 + 1/2O_2 = H_2O + 240\ kJ/mole\ of\ H_2$$

A 1 kg/hr removal of hydrogen by PARS is, from the above, equivalent to ~33 kW introduction of heat into the containment. An addition rate of about 10 MW heat can be anticipated for removal of hydrogen produced in a severe core damage accident when the correct number of AECL PARS units (~75 in a CANDU six building) are installed. This energy addition is enough to fail the containment by overpressure or potentially cause fires if the PARS are operated in high H_2/D_2 concentrations. If recombined with oxygen in a recombiner, only the hydrogen from steam oxidation of Zircaloy in a CANDU-6 single unit reactor will produce over 225 GJ of energy (equivalent to 110 FPS, three hours of decay power at 1%). PARS units at a Bruce/Darlington reactor, if properly sized and populated, will produce about 25% more energy per reactor unit.

The issue of recombiners requires a serious reevaluation but this must wait until a more complete production estimate for Deuterium gas has been established for Bruce and Darlington reactors under severe accident conditions. Given that at present their analyses do not include feeder oxidation and any 'hydrogen' production term Bruce Power / OPG have used for recombiner sizing is likely incomplete. This is an important safety concern. The current design for recombiners at Darlington and Bruce is inadequate, inappropriate and dangerous for these reactors.

Consideration should be given to replace the existing recombiners that are subject to high exit temperatures and hence auto-ignition of the Deuterium rich containment atmosphere by different catalytic plates that inhibit high gas temperatures (Figure 12) by limiting the reaction rates on the catalytic surfaces. Alternately, measures should be undertaken to provide heat sinks to the catalytic recombiners so that gas explosions can be precluded.

The reactor vaults will receive fission products from the disassembling reactor core and hold flammable Deuterium gas with little reason for the gas to distribute to the vacuum building connected from below the reactor vaults (Figure 1, Figure 7). Leakage of Deuterium to the confinement space above the reactor deck cannot be precluded; especially through the seals around pump and steam generator penetrations and the reactivity mechanisms. Burn/detonation of Deuterium mixtures in the confined space under the reactivity deck is facilitated by high local temperatures and ignition plumes from the moderator relief ducts upon dry core debris heatup.

3.8 Deuterium detection systems lacking

Consideration has not been given to installation of enhanced deuterium concentration monitoring systems within containment, process systems and Calandria vessel. On a station basis, the range must include 100% oxidation of Zircaloy at rates consistent with best estimate analyses.

4. ADDITIONAL VULNERABILITIES

Following is a partial list of additional vulnerabilities to an undesirable outcome from a severe core damage accident and are based upon inadequate planning for severe accidents and some CANDU specific features..

4.1 Consequences of recovery actions, such as water addition to the heat transport system upon fuel heatup not evaluated

Evaluation and documentation of the effect of recovery actions including power restoration, water injection as a function of time since onset of core damage needs to be undertaken.

4.2 Consideration of measures for mitigation of consequential fires during the progression of core disassembly

The release of high temperature gases and fission products, aerosols and parts of reactor debris into the confined spaces of the reactor vault from the Calandria vessel relief ducts has potential to cause wide spread fires. This has not been considered in accident management strategies being developed.
Feeder cabinet fires are most likely as the temperatures in the insulated Aluminum wrapped feeder cabinets will rise following fuel heatup on sustained loss of fuel cooling.

This has not been analyzed nor have mitigating measures been taken so that any severe accident mitigation strategies without fire fighting measures will be lacking.

4.3 No advanced instrumentation, monitoring or video systems for severe accident management

There are no video systems for severe accident management and surveillance. Additional instrumentation that can detect and provide critical information specifically designed for anticipated severe accident environmental conditions has not been added. This includes instrumentation to detect and measure Deuterium concentration, radiation monitors, and Calandria vessel water and gas temperature measurements. Critical evaluation of environmental conditions following a severe accident has not been undertaken and this undermines an ability to manage the accidents.

4.4 Installation of emergency hookups for water addition to critical safety and process systems incomplete

A number of opportunities for accident management are potentially missed if the water addition to potential heat sinks and heat transfer pathways is not optimized. For example, water addition to the steam generators can now be only undertaken only after the steam generators have been manually depressurized. Alternate solutions using either steam driven auxiliary feedwater turbines (as installed at Pt. Lepreau) which are passive devices or an upgraded high pressure steam generator emergency coolant addition system (currently a low pressure system) are significantly more effective solutions. The process of depressurization by manual opening of SRVs is not only unreliable but also causes over 40% of the steam generator inventory to be depleted.

Similar considerations should be given to installation of emergency water addition systems for moderator and shield tank water inventories. Current shield tanks do not have a pressure relief valve adequate for boiling under decay heat loads. Neither does the Calandria vessel which must rely upon rupture disks that force loss of up to 15% of the inventory by flashing.

4.5 In-situ design enhancements to avoid Calandria vessel failure not in place

The debris formation in a CANDU reactor is in solid chunks of channel and its eventual retention upon 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 thus introducing water from the shield tank onto hot debris. The effect of Calandria vessel weld failure can vary from additional hydrogen production, accelerated FP releases as one mode of outcome to catastrophic vessel failures by energetic interactions with the hot and molten solid-liquid debris at the bottom of the Calandria vessel as the other mode.

Potential of in-situ design enhancements to avoid Calandria vessel failure by hot debris to avoid catastrophic failure of reactor structures has not been investigated.

4.6 Increased reliability of ECC not implemented

Measures to reduce the likelihood of ECC injection failure after a loss of power have not been investigated

4.7 Consideration of fission product source terms from station wide severe core damage accident lacking

The utilities need to consider full implications of a station blackout scenario that involves progression of a severe core damage accident in all reactor units. The limiting cases of fission product, energy and combustible gas production has not been considered in design of the filtered containment venting system being installed. For high Deuterium concentrations in the containment, likelihood of gas explosions and burns in the filer venting system should be analyzed and precluded for the range of D_2 production amounts.

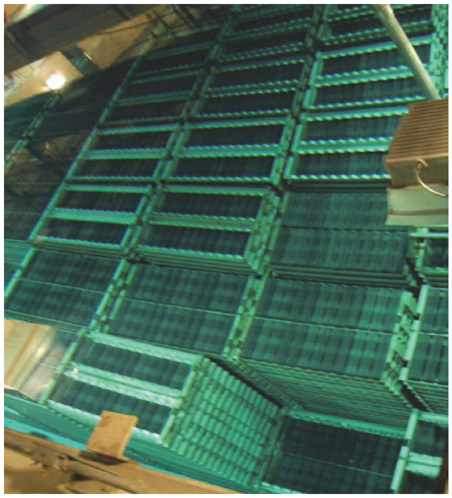
4.8 Accident management strategy development by source term estimates using radiation energy profiles lacking

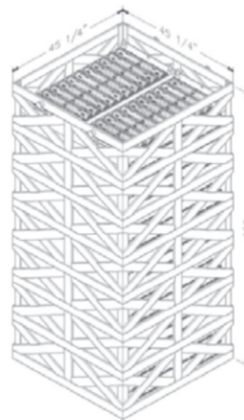
There are no existing methods or instrumentation to help deduce source terms from off-site radiation field measurements (e.g. Reference 9) so that release profiles can be estimated for prediction and radiation effects can be made for different locations and changing weather conditions. This allows prediction of source term from on-site and off-site monitoring in order to predict doses at unmonitored locations and with altered weather conditions. It is a powerful tool for accident management.

There is no on-site and off-site radiation detection equipment that actually detects the source characteristics and differentiates between various incident radiation species by measuring the energy of incident radiation; does not get saturated by incident particulates as happened for Chernobyl at Leningrad station 1000 km away.

4.9 Tightly packed bundles in Spent Fuel Storage susceptible to Zircaloy fires

The fish basket like storage racks do not promote heat removal by air in case of an earthquake induced or malevolent loss of pool inventory and are susceptible to Zircaloy fires. Utilities have undertaken no analyses of consequences of a sustained loss of coolant from spent fuelpools.





4.10 Outdated simulation methods for severe accident progression and consequence assessments

The stations need to obtain a more realistic evaluation of accident progression by using analytical methods that are more modern than the MAAP4-CANDU code that is 25 years old and obsolete in light of new information; and model the event with:

- More detailed modelling of reactor core by differentiating between different bundles by modelling all reactor channels and incore devices
- More appropriate modelling by using D_2O properties instead of H_2O properties
- More appropriate modelling by evaluating Deuterium (D_2) gas production, transport, recombination and burns. Need to consider that Deuterium gas properties differ greatly from hydrogen (H_2)
- Considers oxidation of end fittings and feeders as sources of flammable D2 gas during a severe accident
- Consider a more representative inventory of fission products
- Consider concurrent fires (e.g. In feeder cabinets) as core voids, heats up and degrades
- Consider failure of Calandria vessel at welds with hot debris
- Consider failure of Calandria vessel penetrations at the bottom of the vessel (moderator outlet)
- Consider explosive interaction of water with melt in Calandria vessel
- Consider explosions caused by interaction of Deuterium gas with PARS

4.11 Lack of simulators for operator training on mitigation of severe accidents

Not only are the computer simulation methods for evaluation of progression of severe core damage accidents and consequence assessment outdated, there are no plans or capabilities for development of any simulators for operator training.

5. CONCLUSIONS

CANDU reactors have served well as reliable sources of ~10% of nuclear generation capacity. They were, however, not designed with consideration of severe accidents within their design basis. Fukushima has been a wakeup call to improve the severe accident related vulnerabilities of the 40 year old reactor designs operating around the world. In most cases there is no public airing of the design vulnerabilities and the collusion between the utilities, designers and regulators have kept the issues under wraps. The discussion above of various issues is not an admission of failure but a recognition of the opportunities available for concrete actions to reduce the risk from severe accidents. It is wise to learn from past mistakes and a professional duty of engineers to act in interest of public safety.

6. REFERENCES

1 Improved Regulatory Oversight And Immediate Retrofits For Operating Pressurized Heavy Water Reactors For Beyond Design Basis Accidents, Sunil Nijhawan, ASME paper ICONE20-54387 Proceedings of the 20th International Conference on Nuclear Engineering, ICONE20-POWER2012, July 30- August 3, 2012, Anaheim, California, USA

2 Severe Accident Progression Without Operator Action, Canadian Nuclear Safety Commission, Technical Publication, October 2015. http://www.nuclearsafety.gc.ca/eng/pdfs/Reports/Severe-AccidentProgression-without-Operator-Action.pdf

3 Bruce relicensing hearings transcript, CNSC, 2015-04-15-Hearing-Transcript-edocs4744683-e, page 265, see Vali Tavasoli. http://nuclearsafety.gc.ca/eng/the-commission/pdf/2015-04-15-Hearing-Transcript-edocs4744683-e.pdf

4 Requirements for Containment Systems for CANDU Nuclear Power Plants, A Regulatory Policy Statement. Atomic Energy Regulatory Board document R7, http://nuclearsafety.gc.ca/pubs_catalogue/uploads/R-7E.pdf

5 ROSHNI - A New Integrated Severe Accident Simulations Code For PHWR Level 2 PSA Applications And Severe Accident Simulator Development, Proceedings of the 23rd International Conference on Nuclear Engineering, ICONE23-1054, May 17-21, 2015, Chiba, Japan

6 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, , pp 1023-1028, March 1998.

7 Hydrogen and Deuterium Recombination on a Copper Surface, Surface Science 773 (1997), L333-L338

8. E. A. Reinecke, I. M. Tragsdorf, and K. Gierling, “Studies on innovative hydrogen recombiners as safety devices in the containments of light water reactors,” Nuclear Engineering and Design, vol. 230, no. 1—3, pp. 49–59, 2004.

9. An inverse modeling method to assess the source term of the Fukushima Nuclear Power Plant accident using gamma dose rate observations, O. Saunier et al; Atmos. Chem. Phys, 13, 11403-11421, 2013

ATTACHMENT 3

Proceedings of the 2016 24th International Conference on Nuclear Engineering
ICONE24
June 26-30, 2016, Charlotte, North Carolina

ICONE24-60700

REGULATORY ACTIONS THAT HINDER DEVELOPMENT OF EFFECTIVE RISK REDUCTION MEASURES BY THE NUCLEAR INDUSTRY FOR ENHANCED SEVERE ACCIDENT PREVENTION AND MITIGATION MEASURES AFTER FUKUSHIMA

Sunil Nijhawan, Ph.D, P.Eng.
Prolet Inc.
Toronto, Canada

ABSTRACT

The official report of The Fukushima Nuclear Accident Independent Investigation Commission concluded 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*."

This wakeup call for the nuclear power utilities should require a public review of their relationship with of regulators. However, severe accident related risk reduction is a relatively uncharted territory and given the apparent lack of in-house technical expertise, the regulators are heavily relying on the qualitative and 'hand waving' arguments being presented by the utilities inherently disinterested in further investments they are not required to make under original license conditions. As a result, it has accelerated further deterioration of the safety culture and emboldened many within the regulatory staff to undertake or support otherwise questionable decisions in support of the utilities that prefer status quo. Case in point is the Canadian Nuclear Safety Commission (CNSC) which mostly accepts any and all requests by the nuclear power industry. After Fukushima, the CNSC took a year to publish a set of 'Action Items' for the Canadian Nuclear industry to *prepare plans* over 3 years and then accepted most if not all submissions that in many cases barely addressed the already watered down recommendations. In some cases the solutions proposed by the industry were economically expedient but technically flawed; and some could even be considered dangerous. CNSC also published a study on consequences of a severe accident with a source term that was limited to the desirable safety goal (100 TBq of Cs-137), which coincidently years later matched the utility 'calculations', but orders of magnitude smaller than predicted by independent evaluations. As a result, some well publicized conclusions on the benign nature of consequences of a CANDU severe accident were made and the local and provincial agencies that actually are supposed to prepare off-site emergency measures were left with an incorrect picture of what havoc a severe accident can cause otherwise. CNSC then published a much publicized video highlighting the available operator actions to terminate the accident early and later a report outlining the accident progression for a severe accident without operator action with conclusions that were immediately technically suspect from a variety of aspects. The aim was to claim that a severe core damage accident has no unfavorable off-site consequences. The regulator effectively, in this case, comes across as a promoter for the industry it is legislated to regulate. The paper outlines examples of actions being taken by the regulators that hinder development of effective risk reduction measures by the industry which otherwise would be forced to undertake them if the regulators had not stepped on the plate to bat for them. They vary from letters to editors to silence any safety concerns raised by the public, muzzling of its own staff, trying to silence external specialists who question their wisdom on to blatant disregard for any intervention by public they are required to entertain by law but are accustomed to factually ignore or belittle. The paper also outlines a number of examples of actions that an independent regulator would undertake to reduce the risk and enhance the safety culture. The nuclear regulatory regimes work well generally but in cases where it does not, the results can be disastrous as evident from the events in Japan and as is building up in Canada. The paper also summarizes the disparities between the number of Regulatory Actions instituted by the CNSC against small companies that use nuclear substances for industrial applications and almost none actions against the nuclear power plant utilities it regularly grants a pass in spite of the larger risk their operations pose to public.

INTRODUCTION

Regulatory oversight, guidance and leadership have generally been the driving force in development and operation of innovative and safer reactors worldwide. Some guidance is provided by international organizations such as the IAEA, industry groups and research organizations but the ultimate responsibility for public safety rests with the national regulatory organizations and the utilities that operate the nuclear power plants with the trust extended to them by the public to continually minimize the risk from reactor operation. With a number of serious reactor accidents behind us within barely ~15000 reactor years of operating experience, there is a renewed push for transparent, honest and effective regulatory oversight. Unfortunately that is missing in a number of countries where staff relationships with the utilities trump any information contrary to the business interests of the utilities that the regulators serve. Typically only half the truth comes out – the positive half.

Regulatory regime varies between countries and regulatory involvement in development of engineering and scientific basis for design decisions and the associated basic sciences has been exemplified by the path chosen by regulators such as the US NRC and the independence and force of their decisions. That path is not followed in Canada where the prescriptive regulatory approach is shunned in deference to a more 'consultative' approach. With currently operating reactors sporting a 30-40 year old reactor design there is extreme resistance from the utilities to seemingly expensive upgrades necessary to bring them in compliance with enhanced public expectations, new technical information and emerging knowledge about their vulnerabilities to severe accidents.

In almost all countries there is a legislated, more rigid separation of the utilities that own and operate the reactors and the national regulatory bodies that are empowered to regulate them. In some countries utility executives regularly leave to occupy top regulatory posts and then return to be engaged as consultants. In some cases the regulatory, enforcement and research functions are separated while in others they are intertwined such that enforcement becomes a moving target especially if there is an absence of rulemaking. In a number of cases the regulatory regime works well but in cases where it does not, the results can be disastrous as evident from the events in Japan where a collusion between the utilities and the regulators led to implementation of otherwise questionable decisions not in the best of public interest. Similar dynamics is building up in Canada where the Canadian Nuclear Safety Commission (CNSC) staff is struggling to cope with emerging understanding of severe accident related vulnerabilities in reactors long heralded as invincible symbols of national achievement.

While severe accident analyses work started in Canada in late 1980s, it is lost to the stoic regulators that the design of large number of operating plants, specifically the multi-unit reactors is most vulnerable to severe accidents with potential to cause off-site damage at a national level.

It is not that these regulators are doing nothing. They are making some noise, producing feeble, ambiguous and toothless requirements that do not motivate the industry to effectively look at the methods by which severe accident consequences can be minimized. Level 1 PSA to identify permutations of failures that would lead to a core damage have been done ad nauseam but the next step of understanding the severe accident reactor response and installing mitigating measures from challenges posed by energy, fission product, combustible gas etc has been deferred with claims that such accidents were so improbable that they have trouble 'imagining' them to be credible and worthy of serious examination. Suddenly the probabilistic assessments have no meaning to them and any lessons that they could have learned to not only protect the public better or safeguard the interests of their public stakeholders are suddenly not there.

Regulatory and enforcement functions are handled by the same authority in Canada and their case load includes hundreds of other users of radioactive materials covering Uranium mining as well. There are significant disparities between the number of regulatory actions instituted by the CNSC against small companies that use nuclear substances for industrial applications and the almost zero regulatory actions against the nuclear power plant utilities it regularly grants a pass in spite of the larger risk their operations potentially pose to public. A number of earlier conditions for operating license are at times over ridden quietly in the 'consultative' process (e.g. a pass given to a multi unit station utility allowing it to not pressure test the containment for over 12 years; change the LOCA+LOECC methodology). In-house technical expertise is limited and outdated and the regulators largely rely upon information provided by the utilities to make recommendations to the governing Commission members who go through the motions of holding hearings but rubber stamp almost all requests routinely.

As professional engineers, we should be concerned that alliance emerging between the Canadian regulators and the nuclear power industry may contribute to another Fukushima, this time in densely populated Ontario (population >13 million) where most of the reactors they regulate are located. There are no reasons to suggest that this is limited to Canada.

The Fukushima disaster was supposed to wake us all up and work together to reduce the risk. A number of Fukushima recommendations centered on an overhaul of the regulatory framework were made in the Fukushima report (Reference 1). In particular it recommended that "*In order to prevent future disasters, fundamental reforms must take place. These reforms must cover both the structure of the electric power industry and the structure of the related government and regulatory agencies as well as the operation processes. They must cover both normal and emergency situations*."

Fukushima reminds us that Severe Accidents must be included in the defense-in-depth capabilities of operating power plants or these obsolete reactors must be replaced with modern designs or be phased out. In Canada ten reactor units at 2 multi unit stations are soon to be refurbished at a cost mimicking the cost of new reactors in some countries. The opportunity extended by lessons learnt from Fukushima has been more or less missed at 3 units already refurbished, mainly because of regulatory inaction and industry resistance. Past refurbishment projects have all run late and over budget and the financial impact of yet new design improvements is understandably an unwelcome prospect for the utilities.

A number of national and international organizations undertook, under public and stakeholder pressure, design reviews and came up with plans and guidelines for improving the defense-in-depth. In most cases the reactors were declared 'safe' and minor additions of emergency mitigation measures were made. Some 'stress tests' for European CANDU reactors did even less.

CNSC post Fukushima Action Plan

The CNSC Action plan (Reference 2), published in 2013 with a staggered implementation schedule of 3 years and required utilities submit plans for the following:

- A*n updated evaluation of the capability of bleed condenser / degasser condenser relief valves providing additional evidence that the valves have sufficient capacity.*
- *An assessment of the capability of shield tank/Calandria vault relief capacity.*
- *Assessments of adequacy of the existing means to protect containment integrity.*
- *Installation of PARs as quickly as possible.*
- *An evaluation of the potential for hydrogen generation in the IFB area and the need for hydrogen mitigation.*
- *An evaluation of the structural response of the IFB structure to temperatures in excess of the design temperature, including an assessment of the maximum credible leak rate following any predicted structural damage.*
- *A plan and schedule for optimizing existing provisions (to provide coolant makeup to PHTS, SGs, moderator, etc) and putting in place additional coolant make-up provisions, and supporting analyses.*
- *A detailed plan and schedule for performing assessments of equipment survivability, and a plan and schedule for equipment upgrade where appropriate based on the assessment.*
- *An evaluation of the habitability of control facilities under conditions arising from beyond design- basis and severe accidents. Where applicable, detailed plan and schedule for control facilities upgrades.*
- *An evaluation of the requirements and capabilities for electrical power for key instrumentation and control. A plan and schedule for deployment of identified upgrades. A target of 8 hours without the need for offsite support should be used.*
- *Re-evaluation, using modern calculations and state of the art methods, of the site specific magnitudes of each external event to which the plant may be susceptible.*
- *Where SAMG has not been developed/finalized or fully implemented, provide plans and schedules for completion.*
- *An evaluation of the adequacy of existing modeling of severe accidents in multi-unit stations. The evaluation should provide a functional specification.*
- *Plan and schedule for the development of improved modeling, including any necessary experimental support.*
- *An evaluation of the adequacy of existing emergency plans and programs.*
- *An evaluation of the adequacy of backup power for emergency facilities and equipment.*
- *Identify the external support and resources that may be required during an emergency.*
- *Develop source term and dose modeling tools specific to each NPP.*

A thoughtful evaluation of the CANDU severe accident vulnerabilities would have produced a long, more comprehensive list with firm requirements for actual measures undertaken in a timely manner and not just plans to make plans which have a tendency to be lost in paperwork. But inspite of the long list of watered down requirements listed above, the actual reduction in risk has been minimal.

All Canadian stations have received certifications of their disposition of the above 'Action item' issues but the reality of an actual implementation is quite different. Recall that these were just plans to make plans. In most cases words substituted actions. Industry submissions were never made public but the decision was. It soon became apparent that any and all submissions by the industry were deemed acceptable and the staff eagerly gave pass to all stations with flying colors. An IAEA came soon after and declared Canadian regulatory actions robust and adequate and our reactors safe.

For example, no station upgraded its primary system over pressure relief valves. No station installed hydrogen mitigation system for severe accident source terms. No multi unit station improved on the Calandria vault / shield tank pressure relief capacity. No station installed any new systems for containment integrity enhancements, except for some who installed filtered containment venting systems, albeit without consideration of realistic severe accident source terms. No station installed measures to add water to PHTS at high pressures or any means to manually depressurize the primary cooling system. No station improved on the emergency steam generator coolant addition system to inject at high pressures to avoid a depressurization induced loss of secondary coolant. No station evaluated MCR habitability issues with state of the art computational analyses. No multi unit station performed multi unit severe accident analyses. No station developed credible severe accident source terms for dose evaluations. No new computer simulation methods were developed. No severe accident simulators created for operator training. The list goes on. So little was done but deemed good enough.

Obvious design omissions of the past have been put under the rug or ignored. It was, for example, suggested that the 'hydrogen' source term may be significantly higher than considered as 10 km of carbon steel feeders that connect fuel channels would oxidize at the same time when the fuel heated up under a core cooling degradation scenario. The first reaction by the CNSC staff was a typical knee jerk reaction 'we do not expect the feeders to get **warm**'. As if they had ever even thought about it. Then a later admission upon being chastised was that steel feeders would get hot but not hot enough to oxidize. Six months later their position was that feeder oxidation could now not be precluded but that it would be insignificant. All without doing any analyses. The reality is that feeder oxidation starts at lower temperatures than fuel and the reaction rates are higher by an order of magnitude than for Zircaloy. Fuel gets hot enough (1200^o to 1600^oC) under degraded steam flows to disassemble the Pressure and Calandria tubes, albeit gradually. Feeders, located downstream of the fuel channels in insulated feeder cabinets are bound to get very hot during the process as well. Comprehensive mechanistic analyses undertaken using ROSHNI showed that Deuterium source term from carbon steel would be higher than from intact fuel. This confirmed that a very significant source term for combustible gas (Deuterium actually but the industry has always thought it would be lighter Hydrogen) precluded by the utilities and regulators from consideration of mitigation measures.

Point is that the regulatory staff regularly ignores any new information that would require them to do any more than the base minimum oversight that they now employ. It regularly stretches the truth and uses voodoo science and a 'we know best – we are the regulators' attitude in their public pronouncements to protect status quo rather than do some fundamental thinking. A separate paper documents some of the most bizarre statements and pronouncements by the regulatory staff.

When it was pointed out to CNSC that severe accident analyses undertaken using the now outdated MAAP-CANDU code so far used H_2O properties instead of D_2O, the real cooling and moderation fluid, the reaction from the regulatory staff was that there was to be no appreciable difference in any analytical prediction of consequences. When it was pointed out that D_2 gas would be different than H_2, the issue was set aside by saying that no differences were expected and that a severe accident would produce H_2 anyway (from a D_2O reactor !!!!). When it was pointed out that D_2 recombination by PARS would be different than H_2 recombination the answer was that they knew best and that no differences were expected. Only after repeated public shaming they started a small research program whose preliminary results were initially convoluted to claim differences within instrumentation error. This is just one example of how the regulatory staff resists any interference in their otherwise cozy relationship with the utilities. Obfuscation and demonizing of any external input is a very discomforting standard practice in this industry, although they are required to consider public input by legislation and routinely go through the process, only to take the uniform stance of disagreeing with the interveners, no matter what the issue. All responses to external input, unless laudatory of their actions, are typically in the form of rebuttals.

For 15 years the CNSC had been unable to get the industry to upgrade their critically important primary system relief valves whose inadequate steam relief capacity would lead to an uncontrolled over-pressurization and rupture of the critically important heat transport system pressure boundary. These spring loaded safety relief valves were never designed or tested for steam relief and a loss of heat sinks would lead to their acting as the lone heat sink and relief of D_2O steam. Hand waving arguments by the intransigent utilities were accepted in defiance of the basic ASME BPV Section NB-7000 requirements that the valves for steam service be tested in steam. No Mickey Mouse modelling that has been put forward to justify retention of ill-designed valves and inaction would suffice. That has never been an acceptable approach. Valves are always tested for certification. The latest incredulous claims that the 'model' predictions of relief capacity for the 50 times lighter steam would be ~50% of that for liquid water for which they were designed and tested by the suppliers. Not only would the steam discharge be lower significantly just on thermo-hydraulic principles, the spring loaded SRVs are shown by tests to lift significantly less (25% of the lift for liquid in tests at Wylie Labs for Bruce valves) due to the significantly lower thrust force exerted by the lighter steam.

More frequently than not, it looks like the regulatory staff is totally paralyzed in capture by the utilities that pay its bills and offer other benefits. Public safety be damned. The regulatory commission members who ultimately sign off on the staff recommendations are typically unable to understand the technical issues that form the basis of their decisions and have lately transferred a lot more of the decision making to the senior staff as evident from the latest decision to relicense the Darlington reactors for 10 more years. During this period the reactors would operate at up to unprecedented 235,000 effective full power hours of pressure tube degradation and be subject to expensive refurbishment. Recall that Hydro Quebec management decided to forgo refurbishment and retire the reactors and the CEO of Hydro Quebec Thierry Vandal on January 29, 2013, testified to the Quebec National Assembly as follows: *"I would no more operate Gentilly-2 beyond 210,000 hours than I would climb onto an airplane that does not have its permits and that does not meet the standards. So, it is out of question for us to put anyone, i.e. us, the workers, the public, or the company, in a situation of risk in the nuclear domain. So this deadline of 210,000 hours, this is a hard deadline."* The staff keep extending the safe operation envelope by now talking about a further extension beyond 235,000 hours for tubes whose unplanned hydriding and embrittlement (accelerated corrosion and deuterium pickup by Zr-2.5%Nb, delayed hydride cracking especially near inlet and outlet rolled joints, garter spring failure by embrittlement, etc) is the main cause of premature refurbishment of the CANDU reactors Industry experts have long raised concerns about these decisions (reference 3). It really costs them nothing to take risks with public safety. We all know that none of the regulatory staff in Japan were held responsible for their irresponsible decisions.

Whatever their motives and rewards, many actions and inactions of the regulatory staff is blatantly contrary to public interest they are engaged to safeguard. Their unfortunate and palpable capture by the industry is contrary to public good.

A number of design enhancements have been proposed (e.g. References 4, 5) to better mitigate severe accidents for the operating CANDU plants designed 30-40 years ago without any consideration of severe accidents. As a result of public pressure, the industry and the regulator recently decided to get their own industry group – Candu Owners Group – to adjudicate the proposals. Not exactly an impartial tribunal. The results are as expected. The unspoken conclusion is that reactors are designed by Gods and no improvements are necessary. The utilities disagree with any and every suggestion.

The regulator decided recently to grant the Darlington station owned by Ontario power generation a 10 year license that would go ahead with restoration of an obsolete design at astronomical cost and without any substantial design improvements that would help the operators better mitigate accidents progressing to severe core damage and reduce consequences to the unsuspecting public. A proper action by a responsible regulator would have required utility implementation in newly refurbished reactors of in short order of design enhancements necessary to better mitigate a severe accident and reduce risk. Otherwise no license extensions should have been granted as a continued operation and expensive refurbishment of reactors with obsolete designs cannot be justified.

A WORLD LEADER? A WATCHDOG?

If one just counted the times a national regulator has claimed to be a 'world leader' in its public pronouncements and then critically examined its technical acumen, one would think that the rest of the world is laggard and retarded in its regulatory duties. This delusional self serving pronouncement is far from true and meaningless but dangerous. A simple search of the public hearing documents, presentations and the CNSC website would leave one to believe that we really have a 'world leader' here; an organization of vision.

In almost all presentations made by the CNSC a claim is made of their mandate as a watchdog (with a suitable picture of a bull dog attached occasionally). It is also claimed that they would never compromise safety. The truth of their actions and inactions is quite different and motivations highly suspect.

PUBLICATION AND DISSIMINATION OF INFLATED CLAIMS OF CANDU SAFETY STORY

While we all share our pride in the CANDU technology and routinely celebrate its various achievements, it is important that public safety be paramount not only in our slogans but also in our actions. As engineers we owe it to the society that nurtures us. Reactors of this technology have been employed in 7 different countries, accounting for over 10% of the power reactors world-wide. It is disconcerting to realize that its further development and upgrades are hindered by the utilities and the regulators acting in unison to claim that the reactors are inherently safe without actually critically examining them for challenges that have not been previously considered; just to avoid any design changes or avoid any admission of responsibility. There are many examples but the latest two that relate to severe accidents are reviewed below. Drawing from industry submissions, two recent publications were designed to demonstrate that the reactors afforded significant time for operator action in event of a station blackout leading to a potential severe accident and that any core damage would be a benign event as far as public doses were concerned. These documents, put out with great fanfare, were designed to silence calls for comprehensive environmental assessments and facilitate long term licenses for the Bruce and Darlington multi unit reactors. The following reviews will attest to their actually further retarding growth of safety enhancement measures for nuclear reactor units with obsolete designs.

REVIEW OF STUDY OF CONSEQUENCES OF A HYPOTHETICAL SEVERE NUCLEAR ACCIDENT AND EFFECTIVENESS OF MITIGATION MEASURES

In August 2015, CNSC published a study entitled "Study of Consequences of a Hypothetical Severe Nuclear Accident and Effectiveness of Mitigation Measures" (reference 6). The study concluded:

1. *In this study, where hypothetical severe nuclear accident scenarios were assessed for consequences, there would be no detectable excess risk related to all cancers combined, leukemia and adult thyroid cancer. The only result attributable to the hypothetical accident would be an excess risk of childhood thyroid cancer, largely for the sensitivity cases examined in this study where the GLR source term was increased fourfold.* ***The excess future risk (based on average dose) would be an additional 0.3 percent in developing childhood thyroid cancer*** *(from an approximately 1 percent baseline future risk to a total risk of approximately 1.3 percent) at 12 km from the DNGS for the worst-case scenario.*

2. ***Canadian nuclear power plants are safe****. Following the Fukushima accident, the CNSC Task Force recommendations further strengthened each layer of defence built into the Canadian nuclear power plant design and licensing philosophy to ensure that the likelihood of accidents with serious radiological consequences is extremely low, with an emphasis on severe accidents. In this study, had all of the plant-specific design features, operator actions and other Task Force recommendations been fully credited/realized, the likelihood of a severe accident would have been lowered and the release of radioactive material considered would have*

been significantly reduced. It means that a severe accident would be extremely unlikely to arise or practically eliminated.

There are a number of in-accuracies that immediately make the study suspect.

1. No specific accident scenario was analyzed. None what so ever. An unmitigated station blackout scenario is a standard scenario analyzed in this context worldwide but that was not done.
2. The off-site consequence assessments including prediction of doses was done for a source term of 100 TBq of Cs-137 (without justification) and a corresponding proportional to core inventory amount of some other fission products.

The 100 TBq Cs-137 source term into the environment is really quite small (unless you write it out as 100,000,000,000,000 Bq and be amazed by the number of zeroes) and is equal to one that would come from about 4 fuel bundles of ONE high power fuel channel in a reactor which has 480 fuel channels. The 100 TBq of Cs-137 represents approximately 0.15% of total core inventory of one 2700 MW(th) unit. Actual releases into the atmosphere arising from a unit core inventory of ~80,000 TBq of Cs-137 can be much higher, likely by 2 orders of magnitude. The reasons are simple and summarized below for the reference case of an unmitigated Station blackout scenario in a multi unit plant in Ontario:

1. A severe core damage accident is a plausible event. Initiating events of loss of class IV power have already occurred many times including a transformer explosion in 1993 at Darlington Unit 4 and the Great East Coast blackout of 14 August 2003 that lasted 3 days.
2. Fuel gets hot in a severe accident when channel fluid inventory is depleted.
3. Channel heatup is staggered and sufficient steam for oxidation is available from other channels with delayed heatup and from underlying moderator.
4. Release rates of fission products are high at elevated temperatures. Release rate of Cs-137 could be 1% per minute at 1600°C, so a large fraction will release from fuel and debris into the Calandria in about 4 hours.
5. 'Hydrogen' production from 10 km long, 120 ton carbon steel feeders adds to 'hydrogen' from fuel channels containing ~60,000 kg of Zircaloy and is high enough to case flammable mixtures early.
6. Fission products and hydrogen releases end up in the containment immediately through relief valves and Calandria vessel relief ducts with these releases arriving largely un-attenuated.
7. Multi unit station containment is leaky; has an upto 48% volume per day leakage rate at design pressure at normal temperatures. Elevated temperatures would cause further deterioration of the already leaky containment boundary.
8. Containment is close to atmospheric at onset of core damage with Vacuum Building already 'spent' when fuel heatup starts and will further pressurize due to further energy release into it. Energetic interactions of fuel and debris will present additional challenges and dynamic pressure loads.
9. Containment will pressurize to greater than design pressure easily (0.5 atm for vacuum building; 0.9 atm for reactor buildings) but even leakage into atmosphere at design pressure are upto 2% per hour, orders of magnitude greater than for any PWR.
10. Reactor vessels are attached to the containment pressure boundary and challenges exist for additional breech of containment boundary by melt through of reactor control devices penetrating the containment and deterioration of seals to the critical equipment like pumps and boilers located outside the containment.
11. Combustible Deuterium will be abundantly trapped in the reactor vaults and the overall concentration can be soon higher than for explosive mixtures. Reactor vaults will also directly receive hot gases from hot fuel.
12. Early containment failure due to 'hydrogen' explosions is likely. Current 'hydrogen' mitigation measures designed for orders of concentration of hydrogen are inadequate.
13. Late (< 24 hrs) containment failure due to fuel-water energetic interactions and structural failures is also likely.
14. More than likely a large fraction of fission products will release from containment to environment early.
15. The regulatory limit of 0.15% of Cs-137 releases (less than half a channel worth of fission product inventory) into the atmosphere will be exceeded early.

Authors of the CNSC study pretended long to have done an accident progression analyses and come up with a source term. This was purposely misleading. In an answer to a question at the Bruce relicensing hearings, a CNSC staff even asserted that the 100 TBq source term was far far greater than ever possible by claiming:

> *A "source term" is defined as the types and amounts of radioactive material released to the environment following an accident.*
>
> *For this study, it was based on the magnitude of CNSC's large release safety goal of 1 X 10E14 becquerels of cesium-137, was comparable in magnitude to the 10E-7 type of severe accident scenario discussed by interveners during the Darlington refurbishment environmental assessment and was 4-5 orders of magnitude greater than the actual accident assessed as part of the aforementioned environmental assessment. The source term examined in this study is significantly larger than would be expected under any credible scenario.*

The above implied that the actual source term may actually be lower in a credible accident by 4-5 orders of magnitude than the already low source term of 0.15% of core inventory. A standard comforting answer to confuse the issue but a 4-5 orders of magnitude less than 100 TBq of Cs-137 really is what a gram or so of UO_2 would contain!

This report was presented with great fanfare to the provincial and local personnel who would eventually respond to a real accident off-site. They were sent back with an assurance that fission product releases would be miniscule even if the reactor had the worst imaginable accident, of INES-7 variety. This is an example of how regulatory actions can have a detrimental effect on public safety and emergency preparedness and violate the trust that the public extends to them.

As regulators, CNSC would be aware of the practices regarding source terms just south of the border. But it does not look like that consistency with world practices was the aim. The aim was to trumpet that severe accidents in a CANDU reactor were benign.

Here is what the US NRC has done. What has become known as the NUREG-1465 Source Term has been adapted into regulatory practices through regulatory guide 1.183 (Reference 7) in their defense-in-depth safety philosophy. This document summarizes severe accident radioactive release source terms into the <u>containment</u> by correlating a relationship between details of an accident progression and releases of a number of risk sensitive fission product groups. NRC based it on a major research program it initiated to improve the understanding of likely releases of radionuclides to the containment for accident that progress to severe core damage. The consequences of these radionuclide releases are then first evaluated assuming that the containment remains intact and leaks at the design-basis leak rate. That would soon lead to assuring integrity of tighter containments with 0.1% per day design pressure volumetric leak rates 480 times less than that for Darlington and Bruce multi unit stations that have upto 2% per hour design pressure leak rate; a very weak containment and a reactor system that directly deposits energy, fission products and combustible gases without any attenuation or benefit of a pressure vessel.

The fission product source terms into the containment for LWRs, from NUREG-1465 are summarized below for comparison. Note the large Cesium releases for which the containment must be designed to mitigate and compare it to the claimed 0.15% source term that CNSC claimed for their supposedly superior reactors regulated by a 'world leader'.

Table 1: NUREG-1465 source terms into containment for a severe accident in a PWR

GROUP Title	Elements in Group	Gap Release	Early In-Vessel	Ex-Vessel	Late In-Vessel
Duration (hours)		0.5	1.3	2	10
Noble Gases	Xe, Kr	5.00%	95.00%	0	0
Halogens	I, Br	5.00%	35.0 0%	25.00%	10.00%
Alkali Metals	Cs, Rb	5.00%	25.00%	35.00%	10.00%
Tellurium	Te, Sb, Se	0.00%	5.00%	25.00%	0.50%
Barium, Strontium	Ba, Sr	0.00%	2.00%	10.00%	0.00%
Noble Metals	Ru, Rh, Pd, Mo, Tc, Co	0.00%	0.25%	0.25%	0.00%
Cerium group	Ce, Pu, Np	0.00%	0.05%	0.50%	0.00%
Lanthanides	La, Zr, Nd, Eu, Nb, Pm, Pr, Sm, Y, Cm, Am	0.00%	0.02%	0.50%	0.00%

A CANDU multi unit plant has severe accident related challenges that are significantly more critical than in a typical PWR. A far larger likelihood of containment failure due to hydrogen explosions compounded with absence of a pressure vessel to contain debris combined with a significantly leakier containment, one would assume that the source term evaluations would be a critical element in CNSC regulatory deliberations. It is claimed that the source term into the environment from a leaky, weak containment is so low that there are practically no off-site consequences. As a result environmental assessments become a joke and convincing the Commission to relicense the reactors for long term operation becomes easy. Dissemination of this report by the regulator is thus negligence and complicity of the highest order.

Given that there were no justification for that choice or any solid ground to stand on, a number of interveners protested and following claims were made at different times by the CNSC staff in the last public hearing (reference 8) on the topic:

1. It is the regulatory limit.
2. It is a CANDU specific source term
3. It is a source term that gives the same dose as Fukushima.

Given that the Fukushima dose term was over 16000 TBq, a dose from a similar source term from a CANDU reactor would be 2 orders of magnitude higher if all other conditions that affect source term conversion to dose were the same (distance, wind speed, weather, terrain, etc). It is another matter that Fukushima designs were different and that there was a 24 hour delay in releases into the containment, a 'hold-up' period irrelevant to the CANDU design.
None of the following standard steps necessary to arrive at the source term into the environment were followed:

1. Estimate the inventory of fission products in the core, moderator and the heat transport system.
2. Evaluate progression of a severe core damage accident using a state of the art analytical tool; use dominant accident sequences from probabilistic risk assessment evaluations
3. Estimate the amount of fission product releases from the core components, moderator and the heat transport system
4. Estimate the source term into the containment as a function of time
    a. Identify the release pathways using station specific failure pathways,
    b. Identify and characterize the dominant transport phenomena from degraded core to containment,
    c. Identify and estimate the releases from debris to containment
5. Estimate the in-containment source term as a function of time
    a. Identify and estimate the impact of the retention mechanisms in the containment
    b. Identify and evaluate containment failure modes
6. Correct Severe accident source term into containment for decay
7. Estimate the releases of radioactive fission products, activation products, aerosols and combustible gases from containment into the environment as a function of time.

In another report an attempt was made by CNSC to evaluate accident progression without operator intervention on behest of the Commission president Michael Binder who routinely asks important questions but receives incorrect answers from his staff.

REVIEW OF SEVERE ACCIDENT PROGRESSION WITHOUT OPERATOR ACTION, CNSC REPORT PUBLISHED OCTOBER 2015.

The report (reference 9) published by the CNSC was reportedly based on analyses reportedly undertaken by a utility on progression of a station blackout (loss of all AC power) scenario with no operator action, a scenario that is routinely examined for all reactors world-wide. The report contains alarmingly wrong and misleading conclusions that seem to have been arrived at to serve a different purpose and preordained recommendations. The first is that the boilers remain a heat sink for 5 hours (giving credence to a claim of high probability recovery early in the accident) with an emergency steam generator water supply able to extend the period by another 8-10 hours. The second that the amount of fission product releases into the atmosphere following an unmitigated progression are miraculously only ~0.15% of the total fission product inventory during the first 24 hours, confirming that the severe accident consequences were benign. We should all rest comfortably in that knowledge.

Knowing that for the same scenario of a loss of Class IV and Class III powers that the Darlington Safety Report, published years earlier, claims a steam generator heat sink capability of only 45 minutes, the claim of 5 hours looks suspect. We have verified the 45 minute interval prediction by simple models independently. The claim of 5 hour interval can be reproduced by making some unreasonable assumptions on the amount of water in the boilers, how much of that boiler inventory remains a heat sink and avoiding a number of heat loads. With more realistic parameters, the 5 hour period for boilers to remain a heat sink is a technical impossibility.

A further 8-10 hour claim for steam generator emergency cooling system effectiveness was also made and shown by our analyses to be higher by a factor of 3 than technically and reasonably possible.

Given that I developed the computer code (MAAP-CANDU) that they used, it was easy to detect that a number of easily identified modelling tricks could have been used to arrive at the blatantly suspect conclusions on the long periods of time available for the operators and the miniscule releases from a melting core into the environment from a containment with low design pressure and a leaky structure.

I have reproduced below the technically indefensible 5 hour prediction by assuming an initial inventory secondary side inventory of 328 tons (82 Mg per boiler – something that is higher than possible but long used in the licensing analyses) and assigning only the decay heat from an initial 2650 MWth fission power and considering a small 3 MW constant heat loss from the HTS. This required that a number of additional heat sources, listed later, be not credited and assuming incorrectly that boilers remove heat and maintain thermosyphoning as long as there is any water in them.

Actual boiler dryout time is expected to be about at best 2 hours (and consistent with the 2.27 hours reported in their own Severe Accident Management Guide - SAMG) and this can be easily demonstrated as follows.

Boiler dryout in this context is defined as the time at which thermosyphoning will break down resulting in fast deterioration of heat removal by steam generators. Within minutes the primary coolant will start to re-pressurize and loose its inventory through the safety relief valves (adequacy of whose steam relief capacity is another concern). The 10m height of water within the secondary side of the boilers is a utility established but seemingly conservative point below which the tube surface area is insufficient to promote primary coolant thermosyphoning. My preliminary calculations show that a more realistic prediction of lowest boiler water inventory is when the boiler tubes are about 50% uncovered. Realistically the mass of water in the secondary side can deplete down to about 20 Mg per boiler before boilers are ineffective.

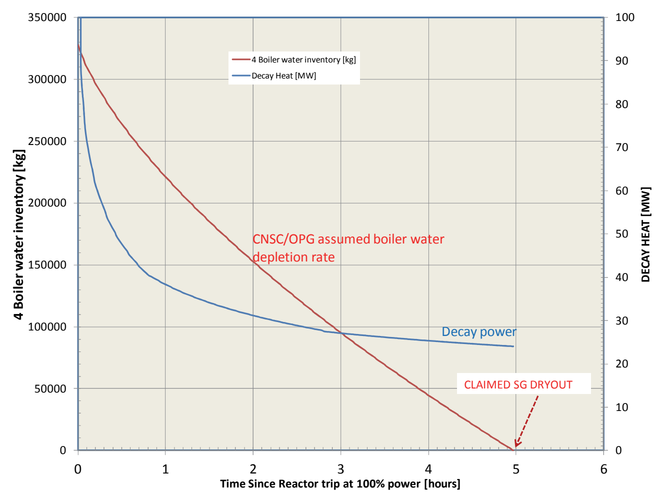


Figure 1 : Boiler boiloff time of 5 hours reproduced for illustration.

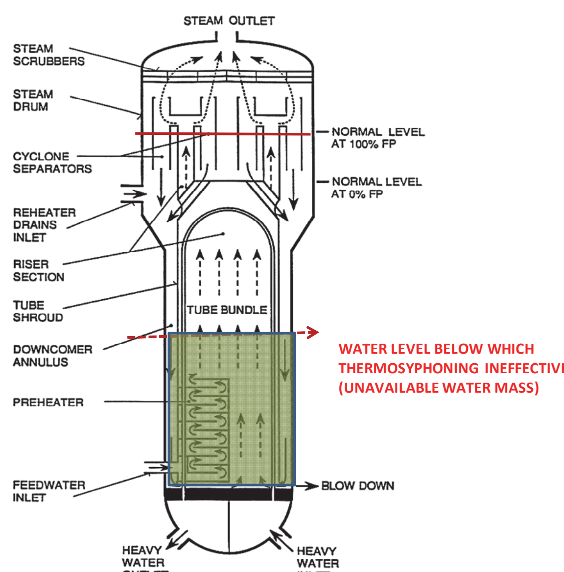


Figure 2: A schematic boiler representation showing water level below which boilers cannot promote thermosyphoning to cool fuel.

Therefore the boilers are not always effective but do not have to be actually dry to zero water mass as assumed by MAAP-CANDU severe accident analysis code which uses an inventory reduction to almost zero to terminate heat removal by secondary side and gives the unrealistic boiler dryout time. For results presented, the conservative limit for breakdown of water depletion to 10m height is also corrected to about 6m.

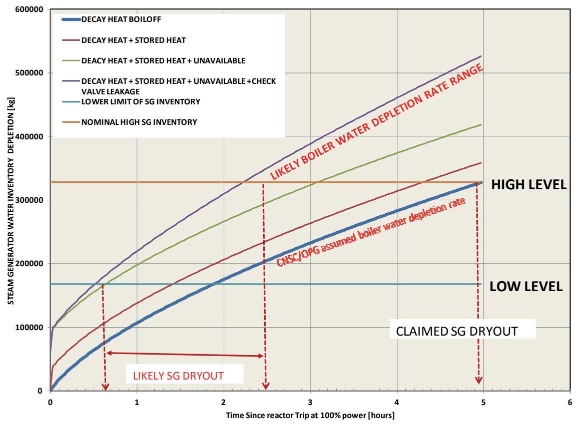


Figure 3: Realistic boiler boiloff time until it cannot remain a heat sink

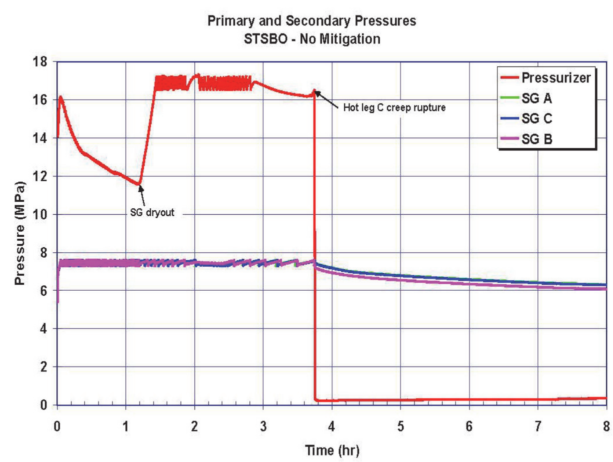
The heat sources and inventory outflows that contribute to accelerated and much earlier secondary side water depletion and seemingly ignored in the MAAP4-CANDU assessment thus are:

1. Stored heat in the fuel. Initial average temperature 880 C. Average temperature following trip is about 290 C. Contribution of cooldown of 133 Mg of fuel UO_2 to depletion of secondary side inventory is about 15.4 Mg.
2. Stored heat in the primary side fluid inventory. Initial average temperature about 300 C. Average temperature following trip – about 290 C. Contribution of cooldown of 185 Mg of primary water to depletion of secondary side inventory is about 9.8 Mg.
3. Stored heat in primary piping. Initial average temperature about 300 C. Average temperature following trip about 290 C. Contribution of cooldown of 200 Mg of metal to depletion of secondary side inventory about 1 Mg.
4. Energy corresponding to residual neutronic energy generation following a reactor trip. Approximately 2.8 FPS for Darlington. Corresponding to secondary side inventory depletion of 4.8 Mg.
5. Feedwater circuit check valve leakage of 1.5 kg/s per boiler. This corresponds to a loss of over 20 Mg over an hour from 4 boilers.
6. Boiler Blowdown flow of 1%/s corresponding to about 13 kg/s (may be as low as 2 kg/s/boiler and terminated upon closure of a valve upon loss of power).

It is important to understand that this period (whether it is 50 minutes or 2 hours) is an important milestone in severe accident management. Once this time has passed and the primary system heats up and depletes its inventory through ruptures or relief valves, no amount of late addition of water to the boilers will ever restore core cooling. A heat transport system with depleted inventory cannot thermosyphon to use boilers as a heat sink and will lead to core degradation.

Thus if were to still to use the MAAP4-CANDU methodology, the effective initial quantity of water is 327-30 (first 4 sources) =297 Mg. In addition, additional depletion by leakage = 40 Mg in 2 hours. Even without consideration of blowdown the heat sink availability is ~2 hours, which is in excess of the 50 minutes in the safety report but significantly less than 5 hours claimed in the CNSC report and the DNGS data from which the number is derived. If the lower bound boiler inventory of 42 Mg/boiler is used, the boilers are an effective heat sink for ~1 hour before HTS begins to repressurize and loose its inventory through the relief valves. Figure 3 shows realistic estimates of boiler 'dryout' time. It is shown that the boilers may cease to be effective heat sinks that promote primary system heat removal by thermo siphoning at about 2 hours.

The Surry reactor is very similar to Darlington in a few important parameters like reactor thermal power (2550 MW Th); That boiler is shown to be effective for only about 1.25 hours in a station blackout scenario (Figure 4, reference 10). The 4 Darlington boilers have the same water inventory at the low boiler level (42 Mg) as the 3 Surry boilers. On the other hand the amount of subcooling required to promote thermo siphoning flows in highly resistive CANDU geometries is higher. Results of boiler inventory depletion analyses are in Figure 4 for Surry boilers.



-28 **Unmitigated STSBO primary and secondary pressures history**
Figure 4: NUREG 7110 prediction of station blackout scenario boiler dryout time of just over 1.25 hours for Surry reactor which is equal in size to a Darlington reactor.

Additional heat sinks by depressurization of boilers and water addition from steam generator emergency cooling system

A claim is made of an additional 8 to 10 hours of heat sink availability following a manual depressurization of boilers and injection of water from Steam generator emergency cooling system. (A tank of water at the top of the reactor building, able to inject 160 tons of water into boilers depressurized to below 500 kPa). This claim is wildly exaggerated and has not been thought through as well. The Steam generator emergency water addition is designed to last 30 minutes when actuated early for the case of a feedwater line or steam line break that depressurizes the boiler. It cannot last 8 to 10 hours just because not all of it can be used and because there is'nt enough of it.

The steam generator emergency cooling system requires Emergency Power Supply (EPS) via Class III bus for control functions and as such cannot be credited unless EPS has been re-established. In addition the system was designed for accidents that depressurize the secondary side (Steam line breaks and feedwater line breaks upstream of the check valves) and as such is ineffective as a heat sink if the boilers are pressurized. The system is designed to provide an alternate source of water for a heat sink lasting 30 minutes.

A manual depressurization of boilers from 5.1 MPa to near atmospheric pressure will result in 31 to 37% of inventory loss from boilers by flashing. Liquid water carryover upon sudden flashing will enhance the inventory loss even further. So no matter what the inventory of the boilers at the time of steam generator depressurization, the forced depressurization induced inventory loss will be significant and can significantly cancel out a large part of heat sink availability by addition of water from the 160 ton inventory in the emergency water tank. Recall that this system requires the boilers to depressurize to less than 800 kPa.

Let us assume that the operator depressurizes the heat transport system at 1 hour. At that time the secondary side inventory may be about 125 tons of water (starting from the incredible 328 tons). A loss of 45 tons of that inventory by flashing (and some more by carryover) will first reduce the boiler inventory to below that required for thermosyphoning and then only provide a benefit of net 115 tons. That amount is good for an additional 90-120 minutes of cooling compared to the operator not taking any action. *To be a good alternate heat sink option, perhaps the emergency water addition system can be modified to operate at higher pressures (>5.1 MPa) for it to be an effective heat sink augmentation source upon a loss of all power.* Given that EPS needs to be established and effective, why would the operator need the Emergency Steam generator water supply anyway? The auxiliary feedwater can be started without the risk of depressurization induced primary system failures.

The regulator made unreasonable claims of time available to the operator to effectively bring in emergency measures in this submission and carelessly went beyond what is documented in the utility SAMGs and what is easily verifiable with simple models.

Fission product source term predictions

The source term predictions of releases into the atmosphere after 2 hours of fuel heatup (calculated after the untenable 5 hours of well cooled fuel) has been presented as about 0.2% of core inventory. That corresponds to releases from less than one fuel channel. This prediction is blatantly underestimated and made to conveniently correspond to the 100 TBq Cs-137 release estimate used in the earlier CNSC report on consequences of a severe core damage accident.

A typical CANDU fuel channel heatup following a loss of cooling is represented in Figure 5. This analysis is for a CANDU6 channel D12 using computer code ROSHNI and captures various stages of boiloff and heatup of a fuel channel following feeder water depletion. It is evident from sample fuel temperatures in Figure 5 and release rates of Figure 8 that the average fuel temperatures in the channel are high enough to permit about 0.1%/min to 1%/min of Cs-137 releases. A Darlington fuel channel will behave no differently and start its heatup not much later.

Onset of channel heatup due to power variations (Figure 6) and feeder water volume variations is staggered as seen from Figure 7; therefore the subsequent channel disassembly is also similarly staggered. Analyses reveal that number of peripheral channels may not fail for 24 hours and the concept of a core collapse and thus immediate cooldown of core materials as used in the CNSC/OPG analyses is now defunct. The core will heatup almost entirely to disassembly in the long run and the fission product release magnitudes will approach 75% before debris melt. Releases into the atmosphere will likely exceed 20% within 24 hours.

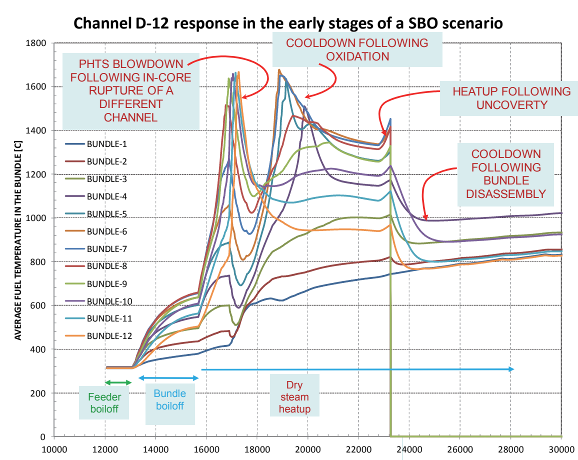


Figure 5: A typical CANDU6 channel thermal response as predicted by severe accident consequence assessment code ROSHNI.

The rate of fission product release from hot fuel is presented in Figure 8 using 2 different widely used correlations. It is evident that for fuel temperatures in the range corresponding to a bundle disassembly at 1200^{o}– 1500^{o}C, the release rates are of the order of 0.1% to 1% per minute. Over the first 24 hours the releases into the containment will be over 50% and releases to the atmosphere well over 20% with high containment leak rates and high likelihood of failure of the relatively weak containment. That is 2 orders of magnitude greater than the ones claimed in the CNSC 'study' entitled Severe Accident Progression Without Operator Action.

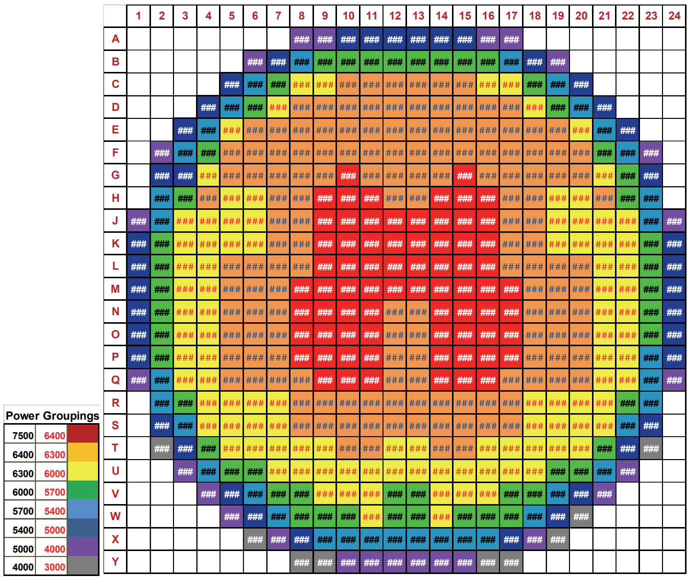


Figure 6: Power variations in a 2700 MW multi unit CANDU reactor

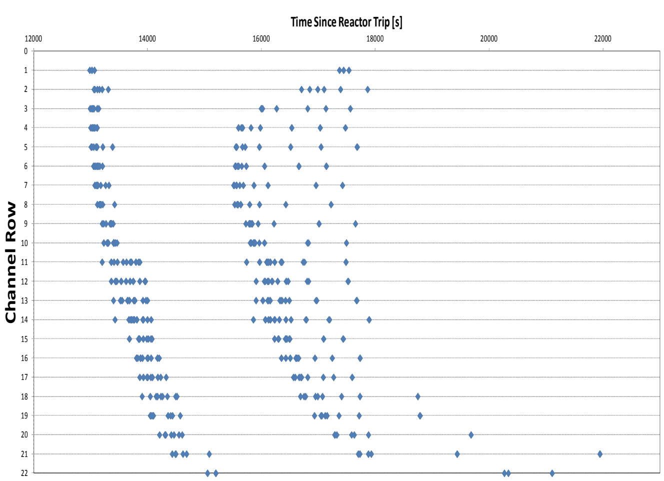


Figure 7: A CANDU6 analysis for onset of channel voiding (left marker) and onset of dry channel heatup (right marker) after boiloff to demonstrate the stagger in core heatup. A staggered channel disassembly will preclude a CNSC report assumed core collapse.

The containment pressurization and failure after 2 hours will result in not only large releases of fission products but also combustible gases that exceed the local flammability limits. The off-site consequences will likely be multiple orders of magnitude higher. Total fission product releases from the channels and debris will easily be greater than 75% and releases into the atmosphere from the failed containment greater than the professed release of 0.2% in the first 24 hours. CNSC should perform independent competent analyses.

Event frequency

The report characterizes an unmitigated station blackout scenario as highly unlikely and the regulator assigns an event frequency of 1E-7/year. The SBO analyses actually represents a large number of events which when binned together have a much larger frequency than for a single event. The consequence assessments represent a large basket of events. For example there have been Loss of Class IV power events at Darlington so the parent initiating event is not of low frequency. For example, On November 25, 1993, a switchyard transformer explosion, resulting in the loss of Class IV power lead to a Unit 4 loss-of-flow event. Class III power loss did not occur. A 3 day east coast blackout in 2003 also caused loss of Class IV power.

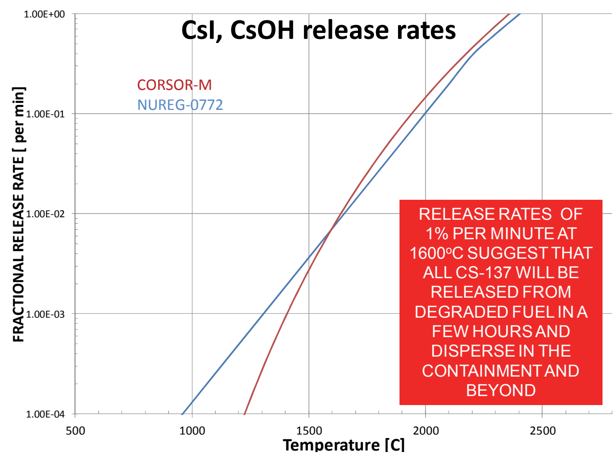


Figure 8: Cs-137 Release rates as a function of fuel temperatures using two different release prediction correlations

The claim of station blackout being a 1E-7 event is borne neither by Canadian PSA nor US data and is not consistent with the established PRAs and in conflict with Darlington PSA results. Results for US PWR Station blackout frequency as summarized in Figure 9 indicate a much higher frequency.

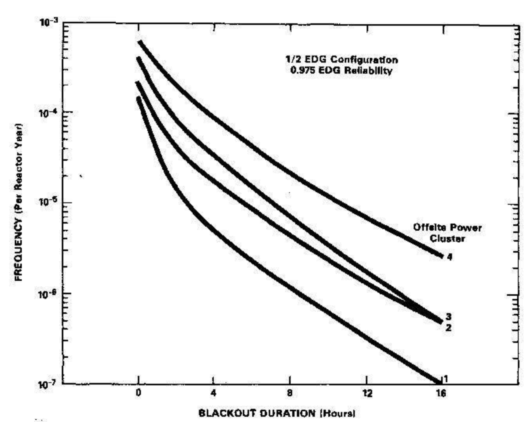


Figure 9: US PWR estimates of a Station Blackout Scenario presented as an illustration of potential range of event frequencies from NUREG-1032.

Early core heatup termination that skews the results

The CNSC/OPG accident scenario includes a convenient early triggering of 'core collapse' option that essentially cools all hot fuel for many hours. This is a convenient assumption that presents a favourable outcome but is not defensible if triggered early by assuming an early bundle disassembly and accumulation of debris. Limitations of the obsolete computer code used to model only 18 fuel channels also come into play. Analyses by more advanced computer code ROSHNI that models each fuel channel in significantly greater detail demonstrate (Figure 7) that individual channel heatup and disassembly will be discreet. We also predict that debris movement to the Calandria water will be gradual without significant long term accumulation. This will result in significantly higher releases from the disassembling fuel. The essentially sold debris will release large amounts of radioactivity prior to melting and a Calandria vessel failure upon its total voiding and failure at welds will further accelerate the process. Off-site consequences will be significantly worse than claimed in the CNSC report.

Combustible gas (Deuterium) production

The report fails to mention anything about the combustible deuterium gas production and its effect on containment integrity. Trapping of 'hydrogen' into the reactor building and ensuing explosions will challenge containment integrity. These failures are not considered. The production of D_2 from reaction of hot steam with feeders may produce over 2000 kg of D_2 and result in early containment failures.

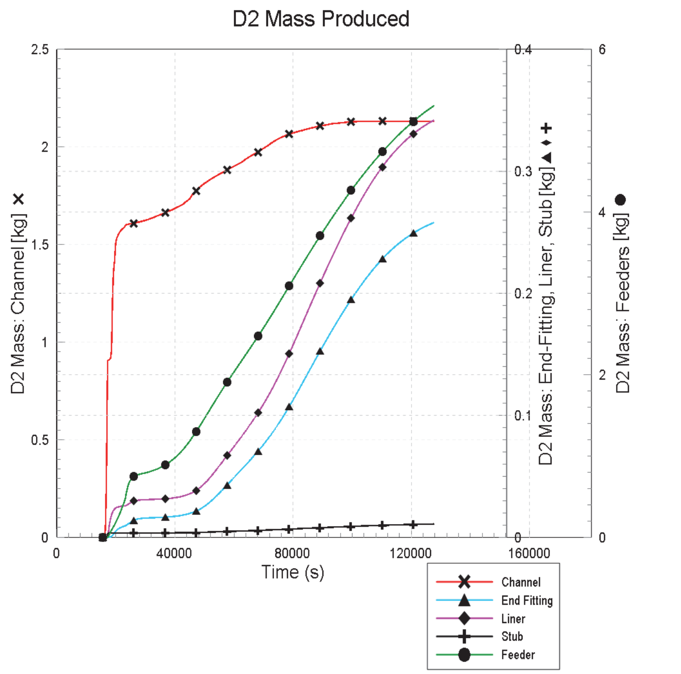


Figure 10: A typical CANDU6 single channel Deuterium gas production during heatup in a SBO scenario.

Figure 10 shows for illustration purposes a CANDU6 channel production of deuterium gas during a Station blackout scenario. A Darlington fuel channel will fare no better or behave any differently. Figure 11 shows early combustible gas production from the core from various sources. Significant and later production of Deuterium gas by debris is not shown. The figure illustrates the combustible gas issue that has been totally ignored in the OPG/CNSC analysis. With such evident disregard for presentation of a complete picture, perhaps the CNSC members should reconsider the merits of the relicensing decision to allow a potential operation of these reactors for another 30 years.

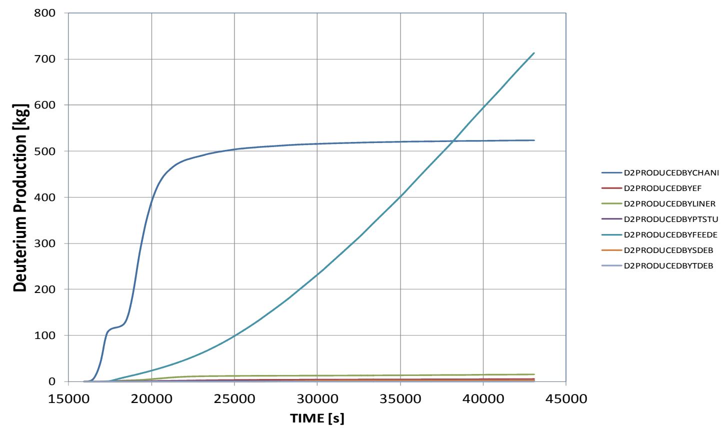


Figure 11: Early production of Deuterium by channels and feeders in a CANDU 6 reactor loop. More D2 is produced later. Idea is to demonstrate the feeder contribution to combustible gas production. Darlington core will produce more.

REGULATORY ACTIONS TO ENFORCE REGULATIONS

Over the last 4 years the regulatory body CNSC has issued over 100 Regulatory actions against small operators and users of radioactive materials in industry. This is done each time with great fanfare and press releases. Not one has been issued against any of the Nuclear Power Reactor operators during that period. Either there are no issues with the utilities or the utilities are considered immune to regulatory action.

Their handling of the November 2009 Alpha contamination event at the Bruce plant (Reference 11) under refurbishment that contaminated ~200 workers is the subject of grave concern, especially to Dr. Greening as summarized in his various submissions at Bruce and Darlington relicensing hearings. The regulator has been unable to find anyone to hold responsible and no substantive actions were taken against the utility. Various reports suggest that the situation was handled poorly. No facilities were available to test the exposure of all the workers for many months. Other utilities were warned only 6 months later in June 2010.

PUBLIC RELATIONS AND BRAND PROTECTION

The CNSC takes great offense to any suggestion that any nuclear activity can be dangerous and writes at least 5 letters a year to the editors of publications that publish any unfavorable concerns about matters nuclear – from uranium mining to Fukushima after-effects. They also routinely herald the limited nature of Fukushima after effects and would rather have us believe that radiation is good for us.

The Commission staff also ensures that no criticism of its activities is undertaken in technical conferences and publications. Case in point is an attempt to get an external author barred from presenting severe accident related issues in Rumania by a regulator VP who insisted jurisdiction over technical discourse in open literature. Note that their muzzling of their own technical staff was the subject of a review as summarized in Reference 12.

CONCLUDING REMARKS

The Canadian regulatory body needs an overhaul. It is possible that similar situation prevails in other jurisdictions as well. It is highly improbable that other reactor designs are superior or that CANDU designs are inferior. It is just that I am more familiar with the PHWR designs. It is up to engineering professionals in their respective countries to raise concerns if they see a similar pattern of regulatory behaviour. Unfortunately we are typically far too burdened to take up the establishment from within the industry. As a pro-nuclear safety analyst I have only scratched the surface of the volume of issues that need disposition and the number of actions that an impartial, competent regulator can take to assure that risk to public is continuously minimized.

The recent reports on the benign nature of a severe accident at a CANDU reactor should be scrapped and fresh independent analyses undertaken in interest of public safety. Reactor upgrades to include severe accident management considerations should be a clear condition of license of any duration. The utilities must realize that what is good for public safety is also good for their own survival. Note that TEPCO will be go bankrupt; Japanese people will suffer for decades but the regulatory staff that conspired to hide the reactor safety issues will never be punished. We cannot afford a Fukushima in Canada and this paper is assembled just due to that fear and 30 years of working on CANDU safety issues, 25 of which have been in severe accident related design reviews and simulation methods development.

REFERENCES

1. The National Diet of Japan, The official report of The Fukushima Nuclear Accident Independent Investigation Commission, Executive Summary, Kiyoshi Kurokawa chairman, 2012

2. CNSC Integrated Action Plan On the Lessons Learned From the Fukushima Daiichi Nuclear Accident, August 2013, http://nuclearsafety.gc.ca/eng/resources/publications/reports/action-plan-fukushima/index.cfm

3. F.R. Greening, April 2014 Submission for Pickering Continued Operation beyond 210,000 EFPH, Canadian Nuclear Safety Commission.

4. Improved Regulatory Oversight And Immediate Retrofits For Operating Pressurized Heavy Water Reactors For Beyond Design Basis Accidents, ASME paper ICONE20- Proceedings of the 20th International Conference on Nuclear Engineering, ICONE20-POWER2012, July 30- August 3, 2012, Anaheim, California, USA

5. Bruce Relicensing hearings, April 2015,

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

7. NRC, "Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors," Regulatory Guide 1.183, July 2000.

8. CNSC public hearings on Darlington Relicensing, November 2-5, 2015. Transcripts at CNSC website.

9. www.nuclearsafety.gc.ca/eng/resources/research/technical-papers-and-articles/2015/2015-severe-accident-progression-without-operator-action.cfm

10. State-of-the-Art Reactor Consequence Analyses Project, Volume 2: Surry Integrated Analysis, NUREG 7110. Jan 2012.

11. CNSC 2010-02-18 Minutes-e-Edocs3531632.pdf.

12. The Big Chill; Silencing Public Interest Science, A Survey, The public Institute of the Public Service of Canada, http://www.pipsc.ca/portal/page/portal/website/issues/science/bigchill