Canadian Nuclear Safety Commission | Commission canadienne de sûreté nucléaire

CMD 15-H8.33A

File / dossier : 6.01.07
Date: 2015-10-19
e-Doc: 4865891

Supplementary Information

Oral presentation

Revised submission from Sunil Nijhawan

Renseignements supplémentaires

Exposé oral

Mémoire révisé de Sunil Nijhawan

In the Matter of

Ontario Power Generation Inc.

Application to renew the Power Reactor Operating licence for the Darlington Nuclear Generating Station

Commission Public Hearing
Part 2

November 2-5, 2015

À l'égard de

Ontario Power Generation Inc.

Demande concernant le renouvellement du permis d'exploitation pour la centrale nucléaire de Darlington

Audience publique de la Commission
Partie 2

2-5 novembre 2015

Canada

Revised Submission to the CNSC Public Hearing on Ontario Power Generation Application to Renew the Reactor Operating Licence for Darlington Nuclear Reactors

Hearing Number Ref. 2015-H-04

19 October 2015

Sunil Nijhawan, Ph.D. P.Eng

SUMMARY

This intervention focuses on the following issues that must be considered in the Commission coming to a thoughtful decision on relicensing of Darlington Nuclear reactors:

1. The requested renewal period of 13 years is unprecedented, far too long and denies the next generation of regulators and concerned public a right of re-examination of an important decision.
2. A proper environmental impact study, especially on the consequences of a severe core damage accident has not been undertaken. The study produced by the CNSC staff is fraught with blatant errors in judgment. It is also dangerously misleading and reflects poorly on OPG understanding of core damage accidents and their potential mitigation.
3. Basic design enhancements that can reduce risk have long been identified for CANDU reactors but have mostly not been implemented at Darlington. The reactors pose an extra-ordinary risk on public and their continued operation without design upgrades so close to the economic heartland of Canada poses undue risk to the national interest.

CNSC commissioners must require OPG to demonstrate that the Darlington 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 12). OPG 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 information presented by OPG is inadequate and the known design upgrades and operator training enhancements lacking.

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.

The intervention also aims to require the CNSC staff to take a more neutral and informed role in the field of severe accidents. CNSC staff is not providing correct information and that the Commissioners of

necessity must rely upon the staff's honesty and expertise because they are not experts and only have a partial understanding of the technical issues. If the honesty and or the expertise of the staff is compromised, then the Commissioners are unable to formulate appropriate conclusions that are truly protective of the health and safety of workers, the public and the environment. The recent reports published by the staff addressing environmental impact of severe accidents are totally unacceptable in quality and content, not to mention the technically laughable conclusions they profess.

The first part of the submission deals with a review of two reports that directly deal with the promised environmental assessment in support of Darlington relicensing. Last week (7 October 2015) the CNSC published a report entitled "Severe Accident Progression Without Operator Action". This report supports an earlier CNSC report on Consequences of a severe accident by 'confirming' that the releases of fission products into the environment over the first 24 hours would be less than 0.2% of the total inventory. I see technical errors that I have discussed in my review. It will be a major travesty if the license renewal was based on the understanding that a severe core damage is a benign event.

Material in the second part of this submission was also submitted in an intervention at the Bruce relicensing hearings in April 2015 and much of that is repeated here because the issues are the same except that OPG and CNSC have produced additional information on severe accidents. Much of that has can be easily discredited and we are back to square one. A Candu Owners Group (COG) task to examine these findings was setup up in July 2015 on behest of the Bruce Power CEO Duncan Hawthorne and CNSC president Michael Binder who showed an uncharacteristic for the industry concern and understanding of the issues I raised at the Bruce hearings. But a COG report has not yet been prepared for discussion or externally issued. Direct interactions with Bruce Power have been in vain as their motivation after being granted an operating license inspite of my intervention seems to have understandably waned. Given that no new action items have yet been agreed upon by the Canadian nuclear industry, the concerns and findings remain the same. Of particular concern is the planned refurbishment of the 4 Darlington reactors without most of the upgrades that are generic to all CANDU reactors, especially the multi unit station at Darlington which supports a relatively weak containment and no proper measures to mitigate the high amount of flammable gases that a severe core damage accident would produce.

SUMMARY OF ISSUES RELATED TO SEVERE ACCIDENT VULNERABILITIES AT DARLINGTON

The operating CANDU reactor units at Darlington nuclear station are housed in multi-unit complex of 4 interconnected containment structures with design pressure retention capacity of less than one bar and an interconnected 'vacuum building' that has not qualified for a multi unit severe accident. While most of the severe accident related vulnerabilities arising from the inherent 40 odd year old PHWR design are common with the single unit CANDU reactors, a station blackout accident at Darlington multi-unit station has the potential of significant off site consequences. Similar to all reactors of that vintage worldwide, the multi-unit reactors at Darlington did not consider severe accidents in the original design. Therefore, they are not unique in requiring serious retrofits in this post Fukushima environment of public expectations of reasonable risk. Some measures to acquire additional backup generators and installation of filtered containment venting systems have been undertaken after Fukushima. However, these measures are at best just good first steps with miles to go.

Planned refurbishments at Darlington station largely do not include any engineered retrofits that can substantially reduce design vulnerabilities and effectively mitigate a severe accident such that effective severe accident mitigation is now a disturbing challenge. A severe accident in all inter-connected units (as by a Station Blackout) can easily become an unmanageable and difficult scenario because of a number of reasons.

The current CANDU design inherently forces reactor damage due to an uncontrolled over-pressurization to pressure boundary rupture even before an emergency injection of water has a chance to act. There neither are any provisions for passive or manual depressurization of the reactor loops after a loss of boiler heat sinks nor a capability for a high pressure coolant injection into the pressurized heat transport loops and an uncontrolled rupture becomes an unnecessary inevitability. An ensuing gradual onset of fuel channel heatup and disassembly puts energy, radioactivity and combustible gases directly into the relatively weak reactor buildings. These structures are quite different from a traditional PWR cylindrical dome building and are rectangular structures built to old industrial standards. The CANDU design also precludes isolated holding of core debris and radioactivity in any vessel like in a BWR, PWR pressure vessel. There are significantly high sources of combustible Deuterium gas ('heavy hydrogen') from large amounts of carbon steel in feeders and Zircaloy in fuel and fuel channels. Given the layout of the reactor units mimicking four inverted volumes interconnected at the bottom by a common duct, separation and accumulation of combustible gases in these unventable inverted cups like geometries makes for impracticable combustible gas control. The small number of Passive Autocatalytic Recombiners planned and/or are installed are neither quantified / qualified for severe accidents nor for the actual gas (Deuterium) they must recombine. There is an enhanced potential for energetic interactions of fuel debris with bodies of water enveloping the hot fuel channels. Pressure relief in relevant reactor systems (PHTS, Calandria, Shield Tank, and Containment) is inadequate for anticipated severe accident loads. With the reactor units directly attached to the containment pressure boundary and a significant number of reactor systems outside the containment, a containment bypass, as for example from reactivity device failure following fuel and debris heatup, is a likely outcome after a severe

core damage. The Calandria Vessel, long heralded as a core catcher, is a thin ~1" thick stainless steel welded low pressure vessel that has been assessed to fail catastrophically at welds and not able to contain hot molten debris. This failure can not only lead to enhanced combustible gas production but also severe energetic explosions leading to failure of structures at the containment pressure boundary. The Shield Tank also cannot contain pressure upon boiling and can fail. Given that unmitigated expulsion of hot gases and fission products targets the small reactor buildings, there is potential for poor equipment survivability. The in-reactor instrumentation for monitoring and control is neither adequate nor qualified for conditions after a severe accident. Severe accident simulation methods are outdated, crude and in dire need of upgrades. There are no dedicated simulators for severe accidents and the perfunctory desktop exercises with high-level Severe Accident Management 'Guidelines' are inadequate. No significant design changes have been implemented since Fukushima that may prevent a severe core damage scenario after a SBO and some well known design problems like inadequate over pressure protection have been ignored. Yet, there are opportunities for engineered upgrades that can substantially eliminate a large number of vulnerabilities. A continued exploitation of an outdated design with refurbishments that extend the life by another couple of decades is not only a risk to public but also to the utilities.

PART 1

Review of Severe Accident Progression Without Operator Action, CNSC Report published October 2015

The report contains alarmingly wrong conclusions. While the amount of information in the report is very limited, there are two major conclusions that are misleading and seem to have been arrived at to serve a different purpose and preordained conclusions. The first is that the boilers remain a heat sink for 5 hours and the second that the amount of fission product releases into the atmosphere are 0.2% of the total fission product inventory during the first 24 hours. Note that the Darlington Safety Report notes a steam generator heat sink capability of 45 minutes only, for the same scenario of a loss of Class IV and Class III powers. We have verified the 45 minute claim. 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 is another pie in the sky.

A number of easily identified modelling tricks are used to arrive at the blatantly suspect conclusions. This from a reactor that has no effective containment for pressure retention or hydrogen mixing and mitigation and a reactor core that has 4 times more Zircaloy and 5 times more carbon steel than any PWR. An onset of severe core damage results in this reactor in direct release of fission products into the containment and a suspect concept of an early quench of core by 'core collapse' that I introduced as a modelling option in the MAAP-CANDU code has been conveniently employed. The analyses are shamelessly self serving and a dangerous indication of the collusion between OPG and CNSC staff to present a picture of accident consequences that is teetering on illegal and immoral behaviour. CNSC has no business repeating licensee's mistakes and should have performed independent confirmatory analyses. Here is some easy to understand analysis.

INITIAL BOILER DRYOUT TIME OF 5 HOURS

The estimate of boiler dryout time of 5 hours is patently wrong and the methodology used to determine this important milestone in progression of a severe core damage accident in the current MAAP4-CANDU is deeply flawed. Actual boiler dryout time is expected to be about at best 2 hours 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 63332-RV25, 26 (whose steam relief capacity is another concern).

The mass of water in the boilers can vary between the nominal mass inventory of 81.8 Mg per boiler for a 4.14 Full Power minute capacity and the FSAR stated lowest operating secondary side mass inventory

at 42 Mg per boiler. The lower limit corresponding to lowest operating water level (SDS2 Low Boiler Level Trip set-point) of 42 Mg per boiler of water inventory is calculated in various sections of the Darlington safety report to approximates the heat sink availability time as 50 minutes even though two important mass inventory depletion mechanisms of 1%/s blow down and 1.5 kg/s check valve leakage were seemingly not considered. The requirement therein was for a 30 minutes worth of heat sink and that was adequately met by the prediction of 50 minutes worth of heat sinks following a loss of Class IV and Class III power.

I have reproduced below the 5 hour prediction by assuming an initial inventory secondary side inventory of 328 tons (82 Mg per boiler) and assigning all decay heat from an initial 2650 MWth fission power and considering 3MW constant heat loss from the HTS. This requires that a number of additional heat sources be not credited and that what seems to have been done to arrive at the 5 hour prediction.

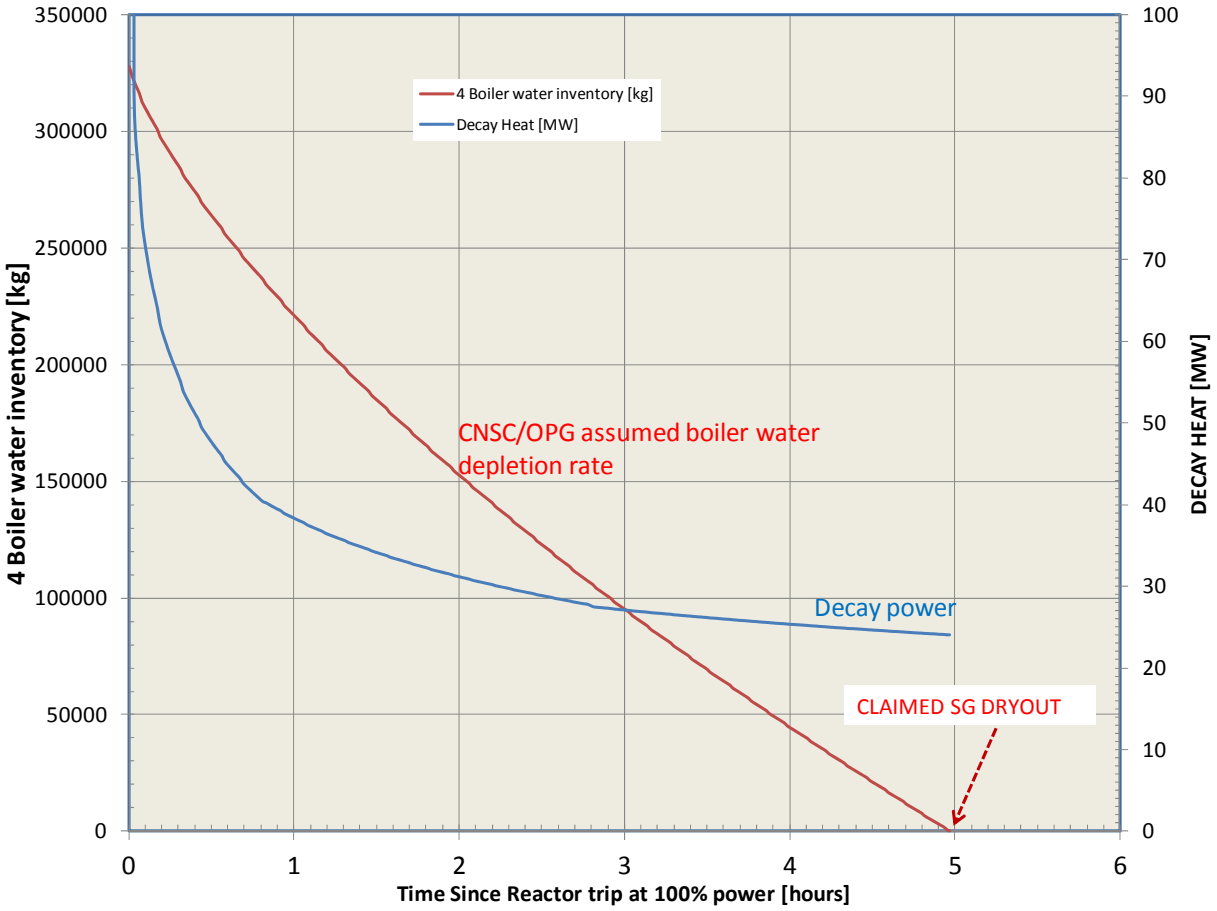


Figure 1 : Boiler boiloff time of 5 hours reproduced for illustration.

While it is debatable whether the 42 Mg of inventory is the correct input for the best estimate calculations, even the upper limit of 82 Mg gives us little help in justifying the wild 5 hour claim.

It is also that critical that two extremely important factors were ignored in MAAP4-CANDU simulations. First is that not all heat sources were considered. Correct methodology is outlined in the Darlington

safety report section 3.3.3.1. Secondly the MAAP4-CANDU method ALSO ignores two important factors for secondary side water inventory depletion (1% constant blowdown {requires a valve to not fail closed upon loss of power} and check valve leakage of 1.5 kg/s per boiler). The heat sources and inventory outflows that contribute to accelerated 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 UO2 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).

The 10m height of water within the secondary side of the boilers is an established point below which the tube surface area is insufficient to promote primary coolant thermosyphoning. See Darlington operator training manuals for confirmation. A fully submerged boiler tube bundle results in a temperature difference of 25 C corresponding to a 7.5 MPa saturated condition in the primary side and 5.6 MPa in the secondary side. A decrease in tube surface area by 50% will result thus in the maximum possible temperature difference of 50C when the primary system has pressurized to above the setpoint of SRV actuation. Thus a reduction of water level to approximately 50% below the top of the boiler tubes will lead to cessation of thermo siphoning and initiate onset of water depletion in the primary side. The mass of water in the secondary side can deplete down to only 15 TO 21 Mg per boiler before boilers are ineffective. Therefore the boilers do not have to be actually dry to zero water mass as assumed by MAAP4-CANDU which uses an inventory reduction to almost zero to terminate heat removal by secondary side.

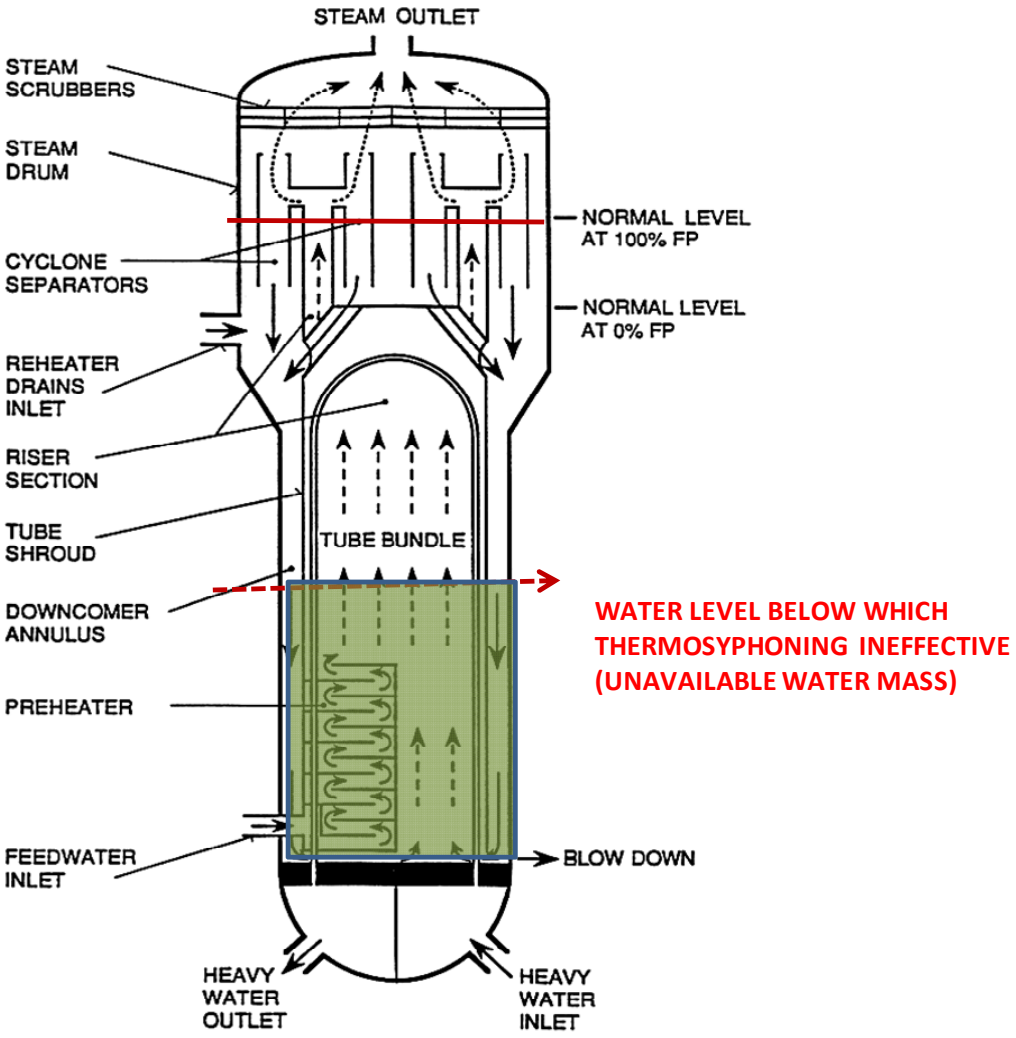


Figure 2: A schematic boiler representation

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.

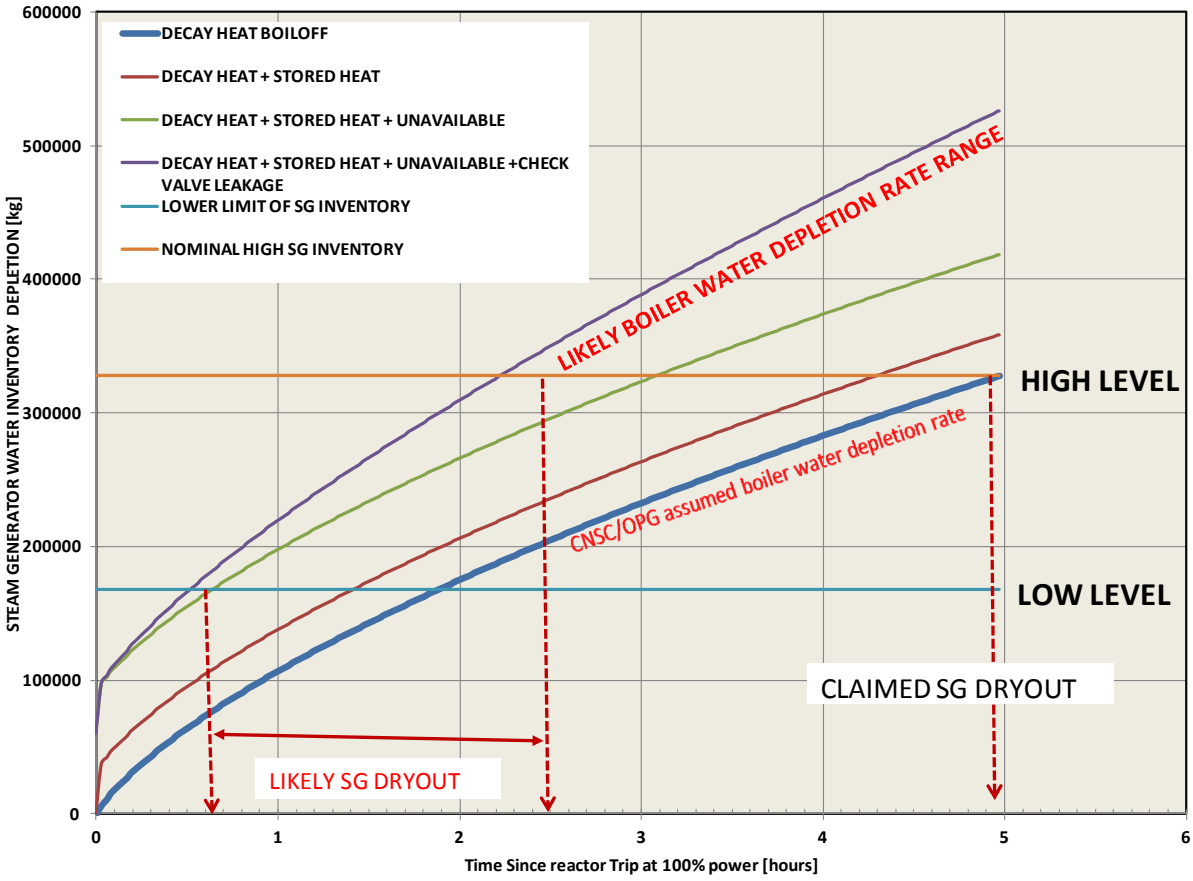


Figure 3: Realistic boiler boiloff time until it cannot remain a heat sink

See NRC published State-of-the-Art Reactor Consequence Analyses Project Volume 2: Surry Integrated Analysis (NUREG/CR-7110, Volume 2, Revision 1). The Surry reactor is very similar to Darlington in a few important parameters like reactor thermal power (2550 MW Th); number of boilers (4). That boiler is shown to be effective for only about 1.25 hours in a station blackout scenario (Figure 4). Darlington boilers have the same water inventory at the low boiler level (42 Mg) as Surry boilers. On the other hand the amount of subcooling required to promote thermo siphoning flows in highly resistive CANDU geometries is higher. Therefore the claim of 5 hours of boiler inventory becomes even more suspect even without doing any analyses. Results of boiler inventory depletion analyses in Figure 3 show that the Darlington boilers will fare worse if the water inventory corresponding to the lowest water level at which boilers operate is used.

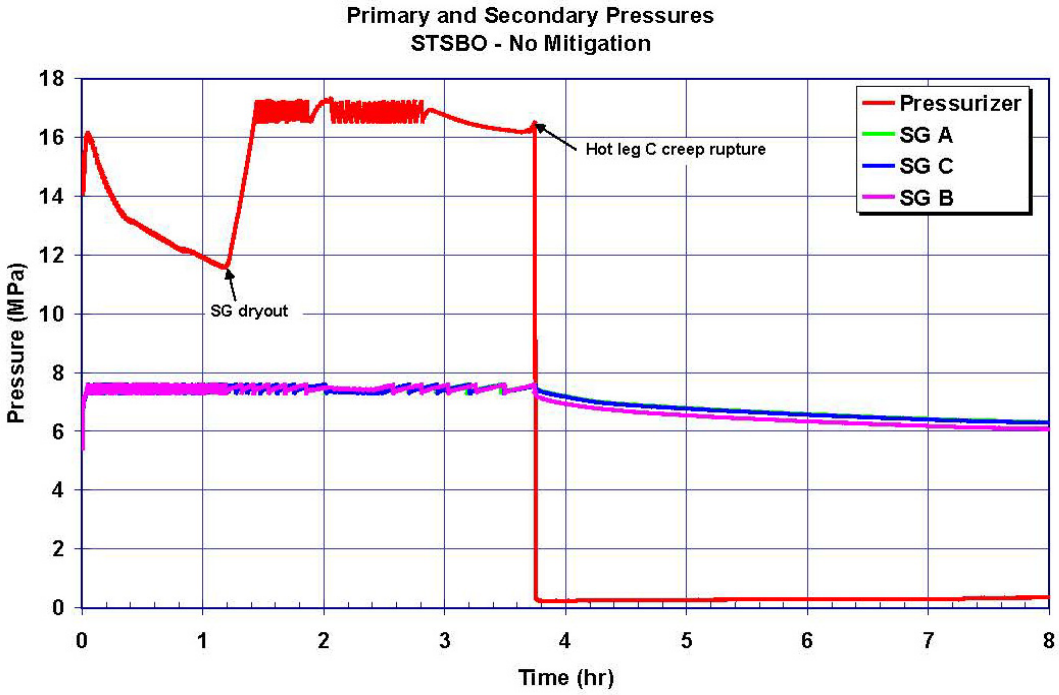


Figure 5-28 Unmitigated STSBO primary and secondary pressures history

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.

That analysis assumed an initial inventory in the boilers of 42 mg each. Darlington boiler will do a bit better at 2 hours (because we have used a higher inventory of 82 Mg per steam generator to represent a 4.14 full power minutes of boiler capacity) but remain in the same range of 1 hours if the 42 Mg inventory corresponding to the low operating level at SDS2 trip setpoint is used. Therefore all remaining predictions for accident progression and consequences including fission product releases in the CNSC report go out the window.

ADDITIONAL HEAT SINKS BY DEPRESSRIZATION OF BOILERS AND WATER ADDITION FROM STEAM GENERATOR EMERGENCY COOLING STSTEM

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. This claim is wildly exaggerated and has not been thought through. The Steam generator emergency water addition is designed to last 30 minutes when actuated EARLY. It cannot last 8 to 10 hours when it is used before boiler level reaches down to the point that the thermo siphoning breaks down...

The steam generator emergency cooling system requires 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 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. 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.

FISSION PRODUCT SOURCE TERM PREDICTIONS

The source term predictions of releases into the atmosphere after 2 hours of fuel heatup 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 correspond to the 100 TBq release estimate used in the CNSC report last year.

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 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.

Onset of channel heatup due to power and feeder water volume variations is staggered as seen from Figure 2; therefore the channel disassembly is also staggered. A number of peripheral channels may never fail and the concept of a core collapse as used in the CNSC/OPG analyses is now defunct. The core will heatup almost entirely to disassembly and the fission product release magnitudes will approach 75% before debris melt. Releases into the atmosphere will exceed 20%.

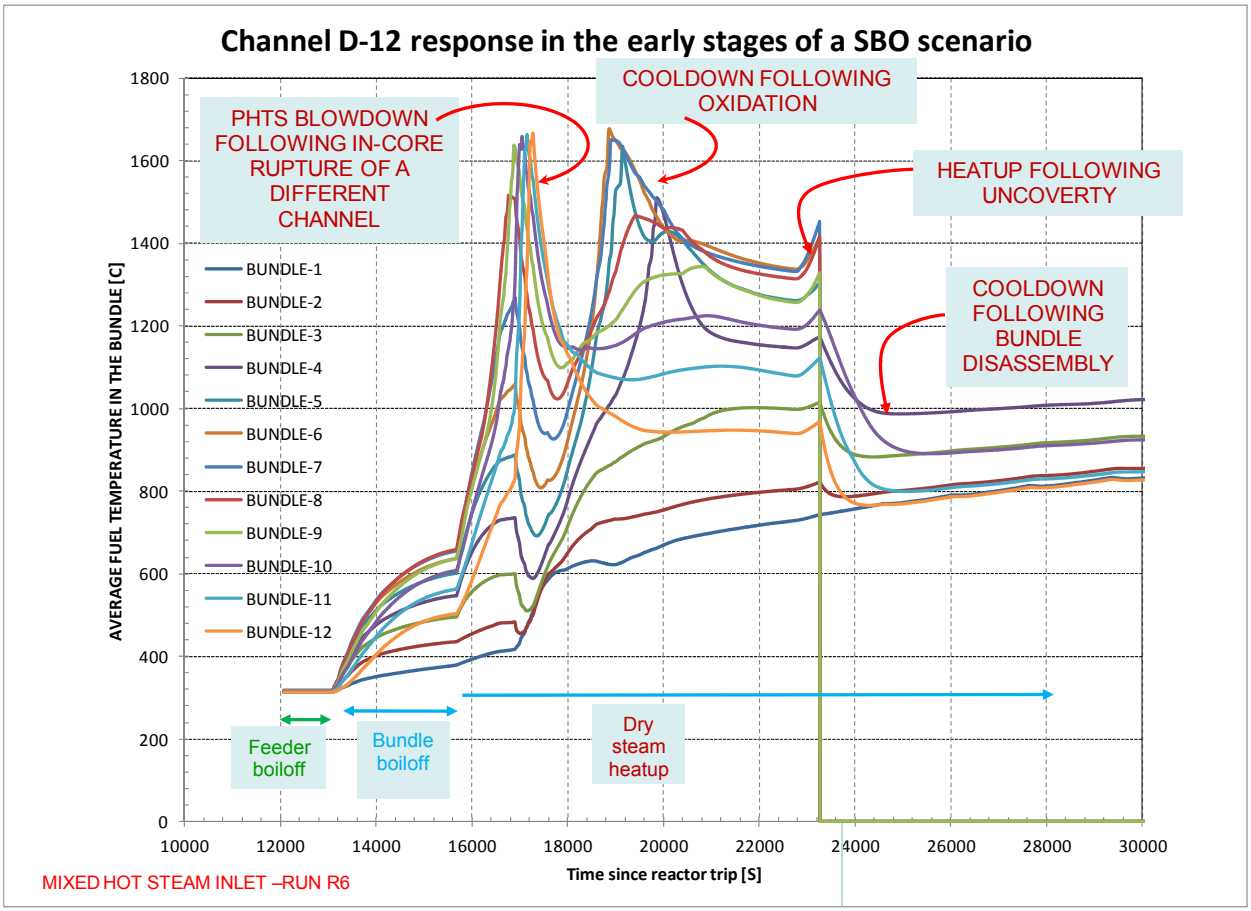


Figure 5: A typical CANDU6 channel thermal response as predicted by severe accident consequence assessment code ROSHNI.

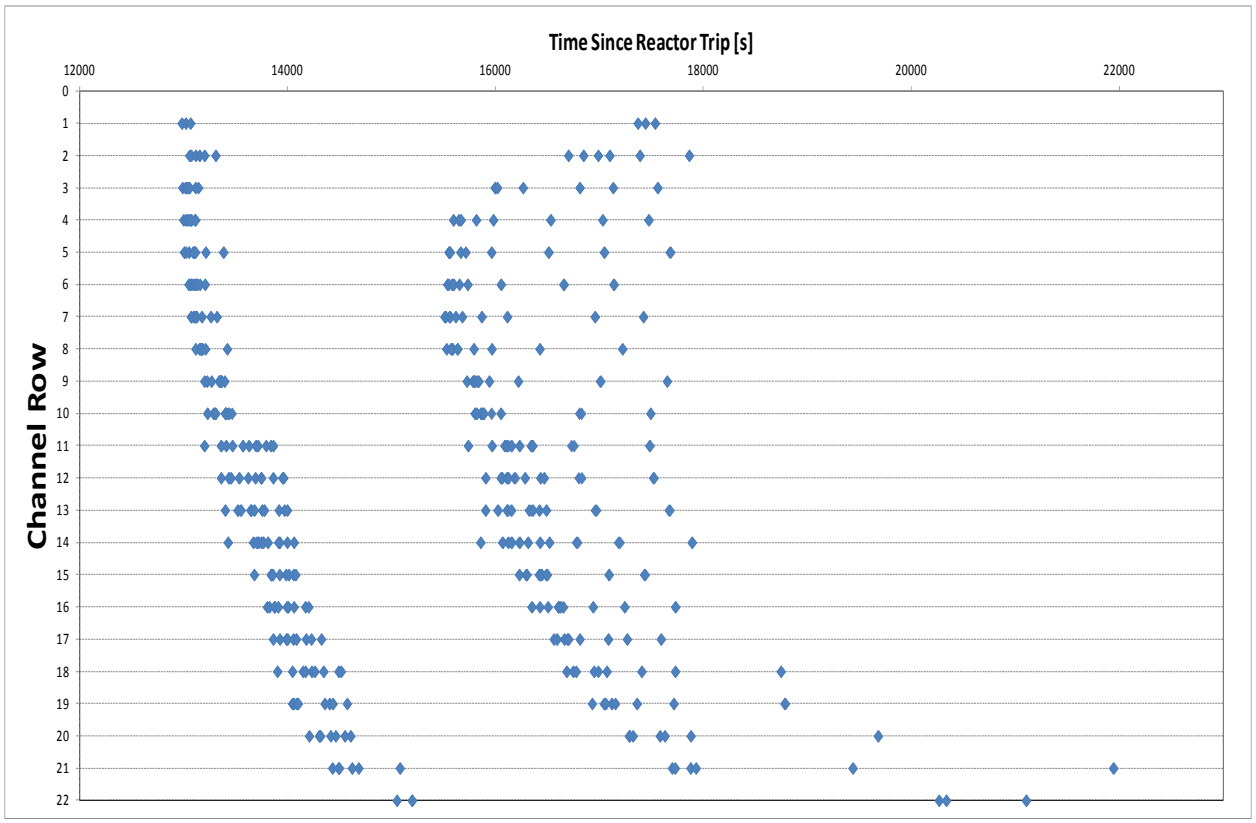


Figure 6: A CANDU6 analysis for onset of channel heatup after boiloff to demonstrate the stagger in core heatup. A staggered disassembly will preclude a core collapse.

The rate of fission product release from hot fuel is presented in Figure 7 and Figure 8. It is evident that for fuel temperatures in the range corresponding to a bundle disassembly at 1200 – 1500 C, the release rates are high and 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 over 20%. That is 2 orders of magnitude greater than the ones claimed in the CNSC 'study'.

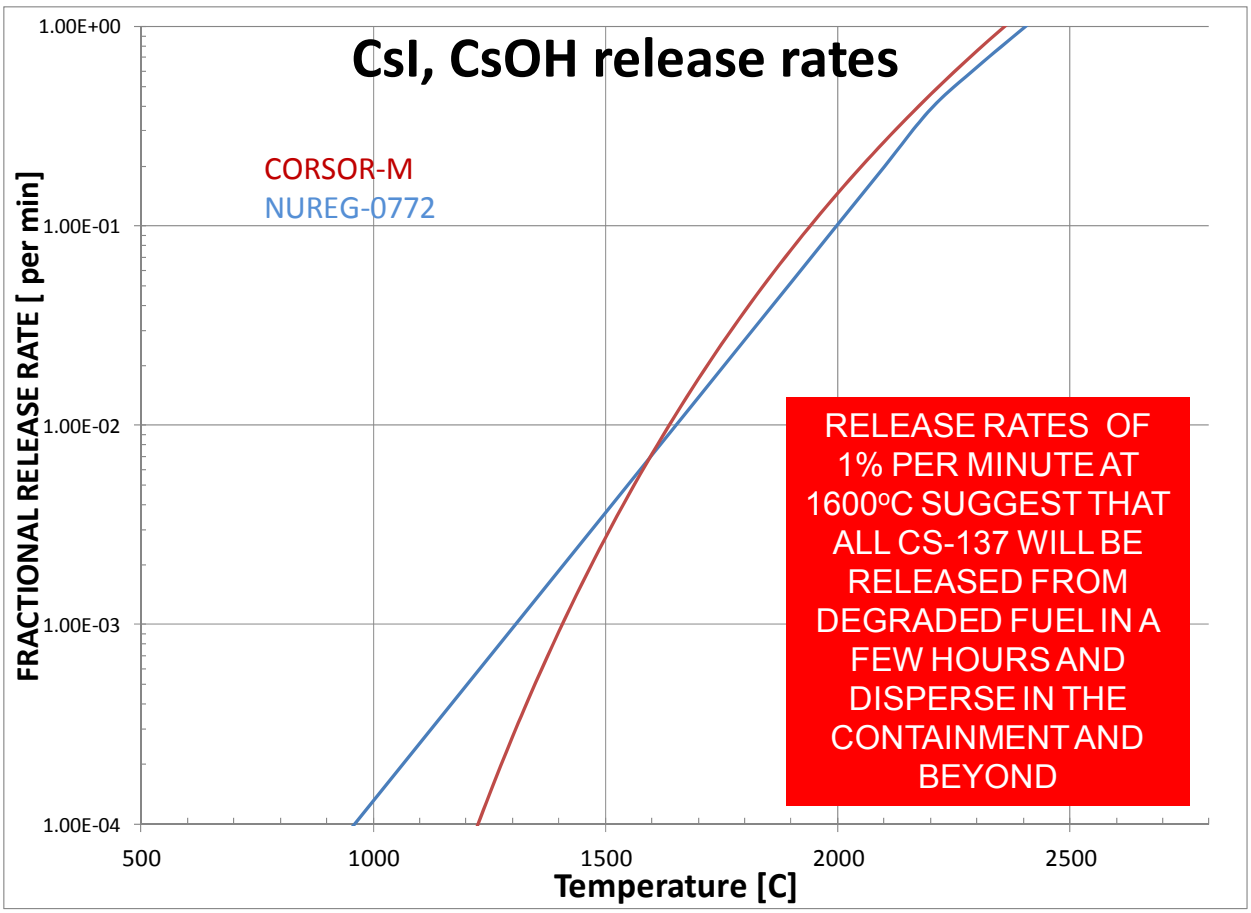


Figure 7: Cs-137 Release rates as a function of fuel temperatures using two different release prediction correlations

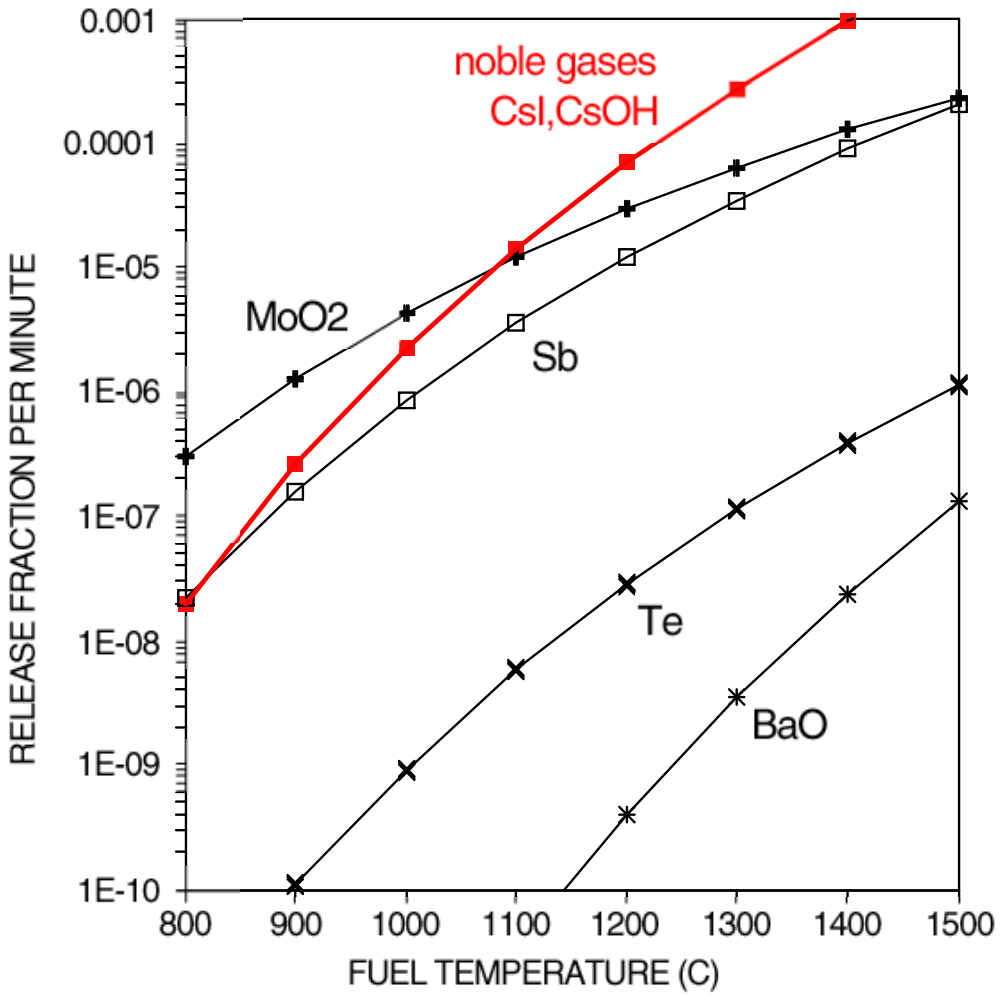


Figure 8: Release predictions for a number of fission product species as a function of temperature.

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 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 a station blackout scenario as highly unlikely and assigns an event frequency of 1E-7/year. The SBO analyses actually represents a large number of events which when binned together have a larger frequency. The consequence assessments represent an even large basket of events. For

example there have been loss of Class IV 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.

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 PWRs as summarized in figures below indicate a much higher frequency.

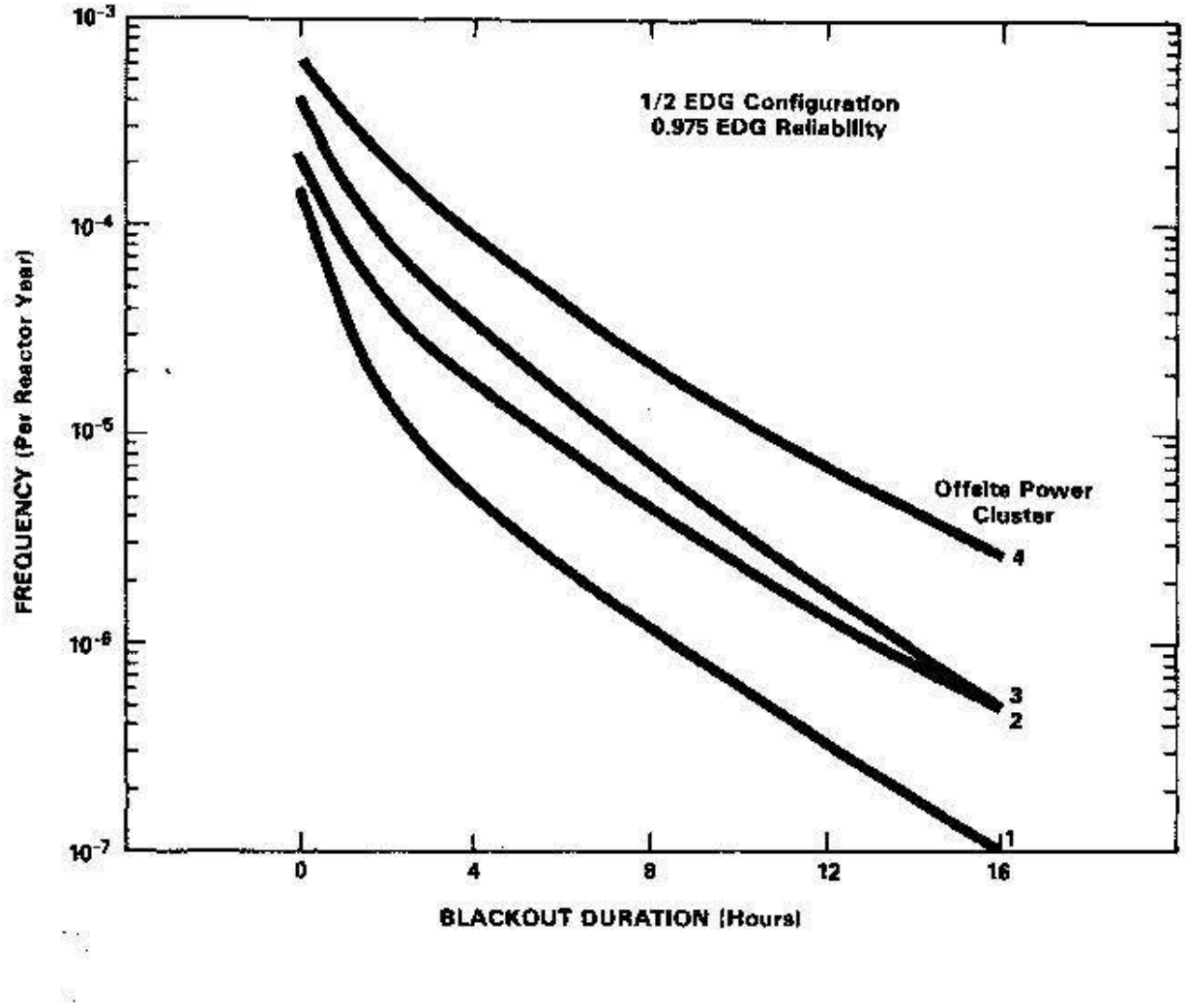


Figure 5.1 Estimated frequency of station blackout exceeding specified durations for several representative offsite power clusters

NUREG-1032 5-2

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

SCENARIO CHARACTERIZATION

The accident scenario includes a convenient prediction of core collapse that essentially cools all hot fuel for many hours. This is a convenient assumption that presents a favourable outcome but is not defensible. Analyses by more advanced computer code ROSHNI demonstrate that individual channel disassembly will be discreet and debris movement to the Calandria water will be gradual without significant 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 will accelerate the process. Off-site consequences will be significantly worse than predicted.

COMBUSTIBLE GAS 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 D2 from reaction of hot steam with feeders may produce over 2000 kg of D2.

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. Figure 11 shows gas production from the core from various sources. Significant 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 application.

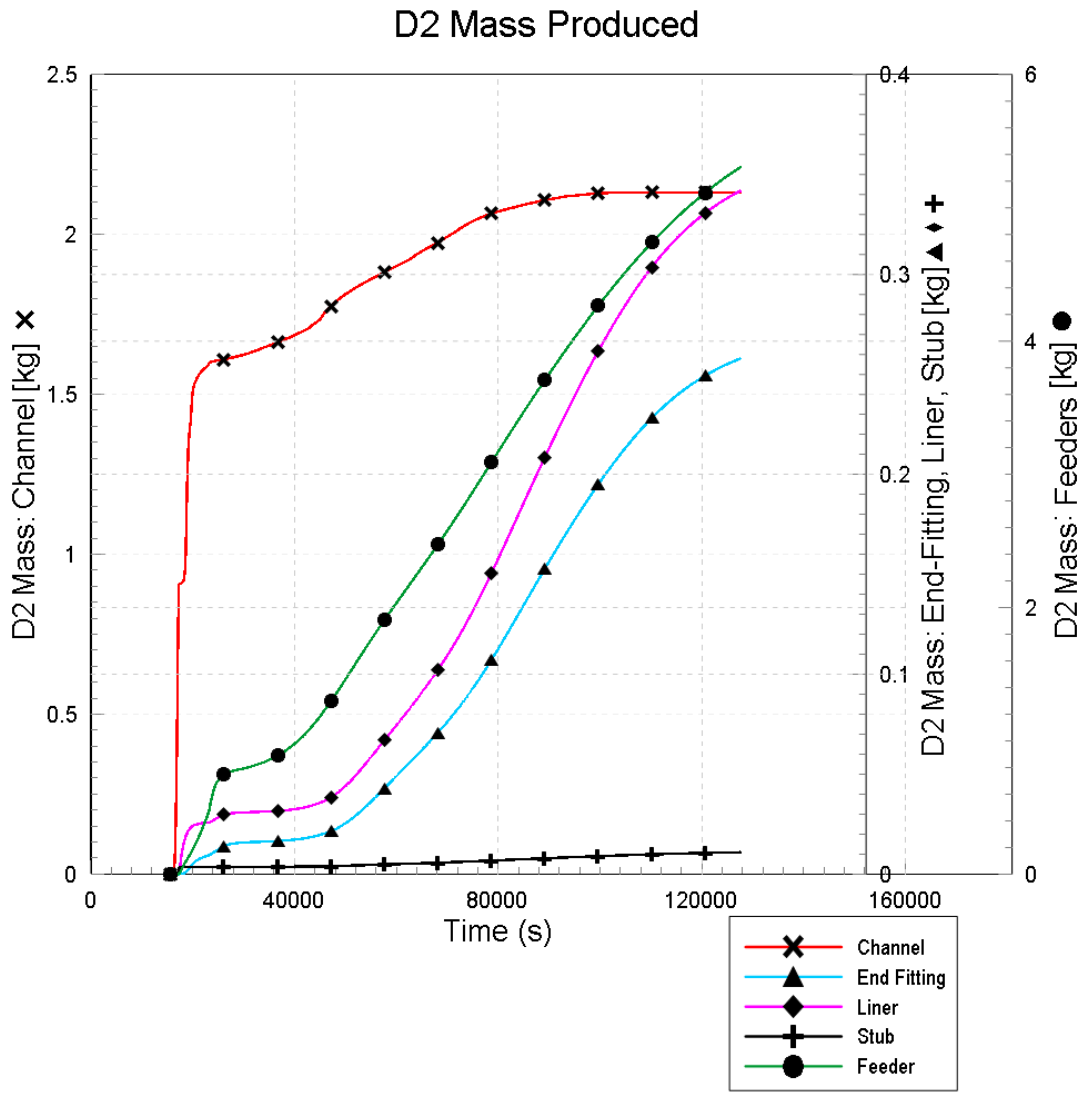


Figure 10: A typical CANDU6 single channel Deuterium gas production during heatup in a SBO scenario.

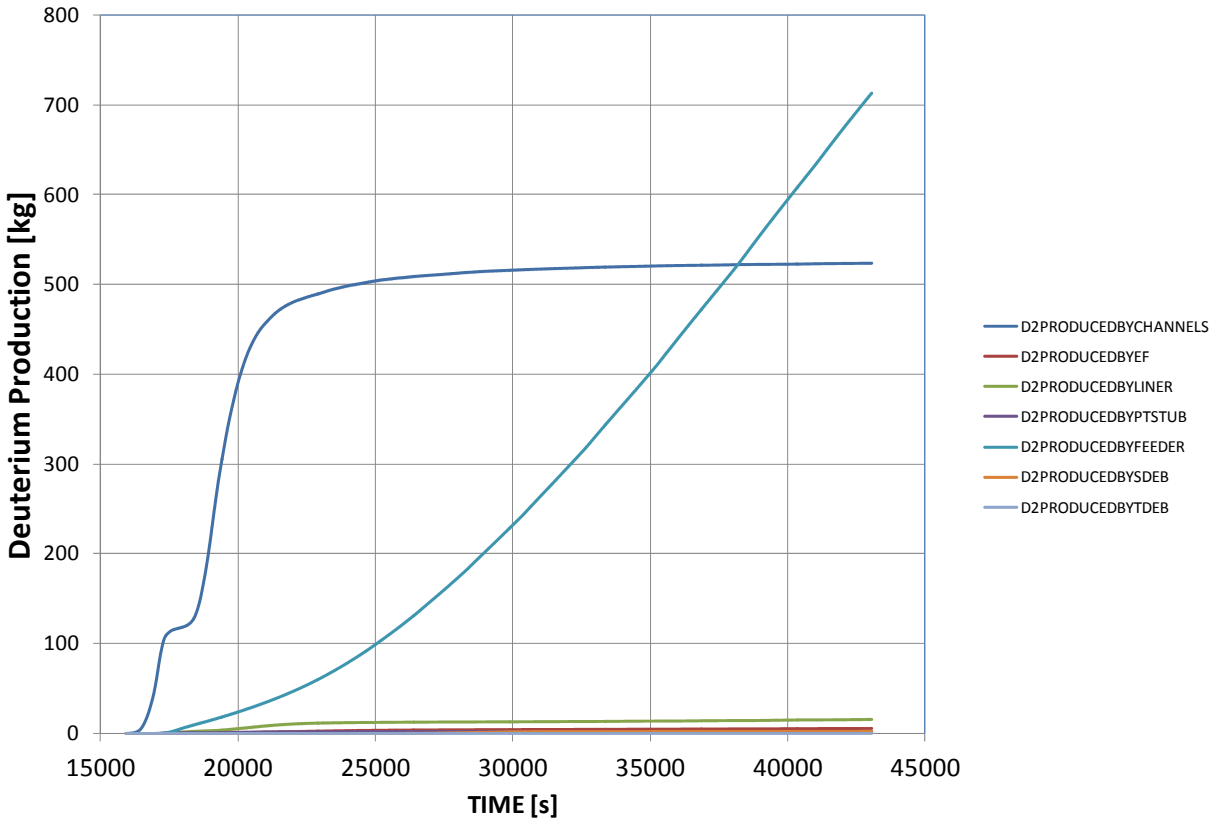


Figure 11: Early production of Deuterium by channels and feeders in a CANDU 6 reactor loop. More D2 is produced later. Idea is to demonstrate the feeder contribution to combustible gas production. Darlington core will produce more.

RECOMMENDATION

The report should be scrapped and fresh independent analyses undertaken in interest of public safety. This should be a clear condition of license of any duration.

PART 2

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 (reference1) 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.*

A review of the CNSC study on consequences of a severe accident in a nuclear reactor published in August 2015 makes apparent now that the CNSC staff have ceased to be impartial and are colluding with OPG in mis representing the consequences of a low probability, high consequence accident as took place unfortunately but not unpredictably in Fukushima.

The following conclusions on the root causes of the Fukushima accident (reference2) seem to apply to the CNSC and OPG as well:

- 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

The recommendations of the Fukushima report should be properly dispositioned for Darlington as well:

- 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 Darlington 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. The refurbishment projects should be put on hold until an improved design of the reactors and support measures has been implemented.

Unless the Commission members and OPG management totally absolve themselves of the responsibility vested in them, necessary upgrades to Darlington 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 and refurbishment 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 OPG CONTINUED OPERATION OF DARLINGTON NUCLEAR REACTORS

While it is recognized that Darlington nuclear power plant units 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. Of particular importance is the effect a disruption in the immediate vicinity of Darlington will have on Canadian national economy should be properly examined.

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 not be undertaken and any licence renewals must be based on completion of risk reduction, not on promises of making plans to do so.

If OPG management 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 (~2 years). 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). OPG 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 42) 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.

I produced the very first report on Darlington severe accident progression and consequences in 1988 and helped identify the design flaws that plague this design. Those who understand principles of reactor safety and licensing will also tell you that the Darlington CANDU 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 Darlington 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 these Clarington reactors of a sustained and

[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)

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 (less one atmosphere gage design pressure) with layout that promotes high local concentrations of flammable Deuterium (also called heavy hydrogen by the uninitiated) 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.

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 Darlington 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 (OPG & 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 OPG is again rubber stamped licence extension for an unprecedented 13 year period 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 DARLINGTON 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 the 4 Darlington units 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 17 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 multiyear 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. Ontario is ill served by OPG 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 Darlington reactors. The PSA numbers presented in the Ontario Power Generation submission mean nothing as 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 Ontario Power Generation. We cannot

[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. The August 2015 values which are 2% larger are impossible to justify.

accept the risk from continued operation of Darlington reactors without its quantification by Ontario Power Generation and verification by independent experts.

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 Darlington 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 Darlington 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 Darlington[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 Darlington 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 side inventory falls too low to remove heat from the thermo-syphoning water flowing in fuel channels (~2 hours without crediting operator action to use deaerator inventory and corresponding to a remaining inventory that covers less than 10m) 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*

[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).

safety relief valves confirm this) leads to a continued over pressurization. These pressure relief valves were reportedly properly designed in the original CANDU units but erroneously mis-sized in 1996 after a knee jerk reaction (and poor engineering decision) to a 1995 event at Pickering.

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 Darlington. 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 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 15*), 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 16 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 Darlington 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 19 *shows that the fission product release from overheated fuel may be fast and 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.*

Darlington 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 13*) 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 certain amounts 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 Darlington there is no pressurizable containment as the reactors are housed in quasi industrial buildings (design pressure < 97 kPa(g)= 95% 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 13*) 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 Darlington 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 14 .

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 13*). 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 1.5 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. Upgrades to the Darlington shield tanks were discussed and may have been implemented.

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 Darlington 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. Ontario Power Generation liability and damage to environment becomes unfathomable. See page 36 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 . Commission should ask for Darlington experience in testing these valves.*

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 150 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 OPG 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 Darlington 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. Small scale experiments at CRL have shown that the gases behave differently.

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 15). These will produce more combustible deuterium. The small (<100 kmole) source term 'hydrogen' for LOCA+LOECC in the safety reports is amusingly wrong. Ontario Power Generation 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% Deuterium 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 Deuterium 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 18). 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. The claim by the CNSC staff at the August 2015 Darlington hearings that any differences observed between Deuterium and hydrogen at recent incomplete investigations at CNL may be within the instrumentation errors is alarming, premature and consistent with their previous lack of understanding of the issue.

[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.

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;

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

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 Darlington 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 OPG 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.

Darlington NGS 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 20), 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 Darlington 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. The rated steam relief capacity has not been determined but as the valves are rated for liquid relief;

Rated Liquid relief capacity = 100 l/s at 290^{o} C.

OPG Reported Steam relief capacity in 2003 = 1.5 kg/s at relief set point

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 ~30 kg/s as the decay heat equivalent for a Darlington 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 23) 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 Darlington reactor is about 30 MW or 30 kg/s of steam equivalent. For a typical PWR that is also 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 pressure in the system at the set point of the safety relief valves (Figure 21), while the CANDU steam relief capacity from 2 SRVs is capped at 4 kg/s will result in an uncontrolled rupture (Figure 22). 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 was 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 Darlington SRVs were actually designed for **liquid** relief of about 100 kg/s and a steam relief of less than 2 kg/s as per their submissions to the CNSC. 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 24) 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 Ontario Power Generation misinformed about steam relief capacity for 10 years and the CNSC staff assigned to the task was 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, it 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 DARLINGTON SEVERE ACCIDENT PROGRESSION & MITIGATION ISSUES

- Darlington 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 Darlington designs inherently forces 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 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)
- Darlington 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 ONTARIO POWER GENERATION 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. SINCE THE LICENCE RENEWAL COVERS REFURBISHMENT OF DARLINGTON UNITS AT A GREAT COST, 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 Darlington; with the realist in me knowing better and fearing for those living close to Darlington 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 19 October 2015.

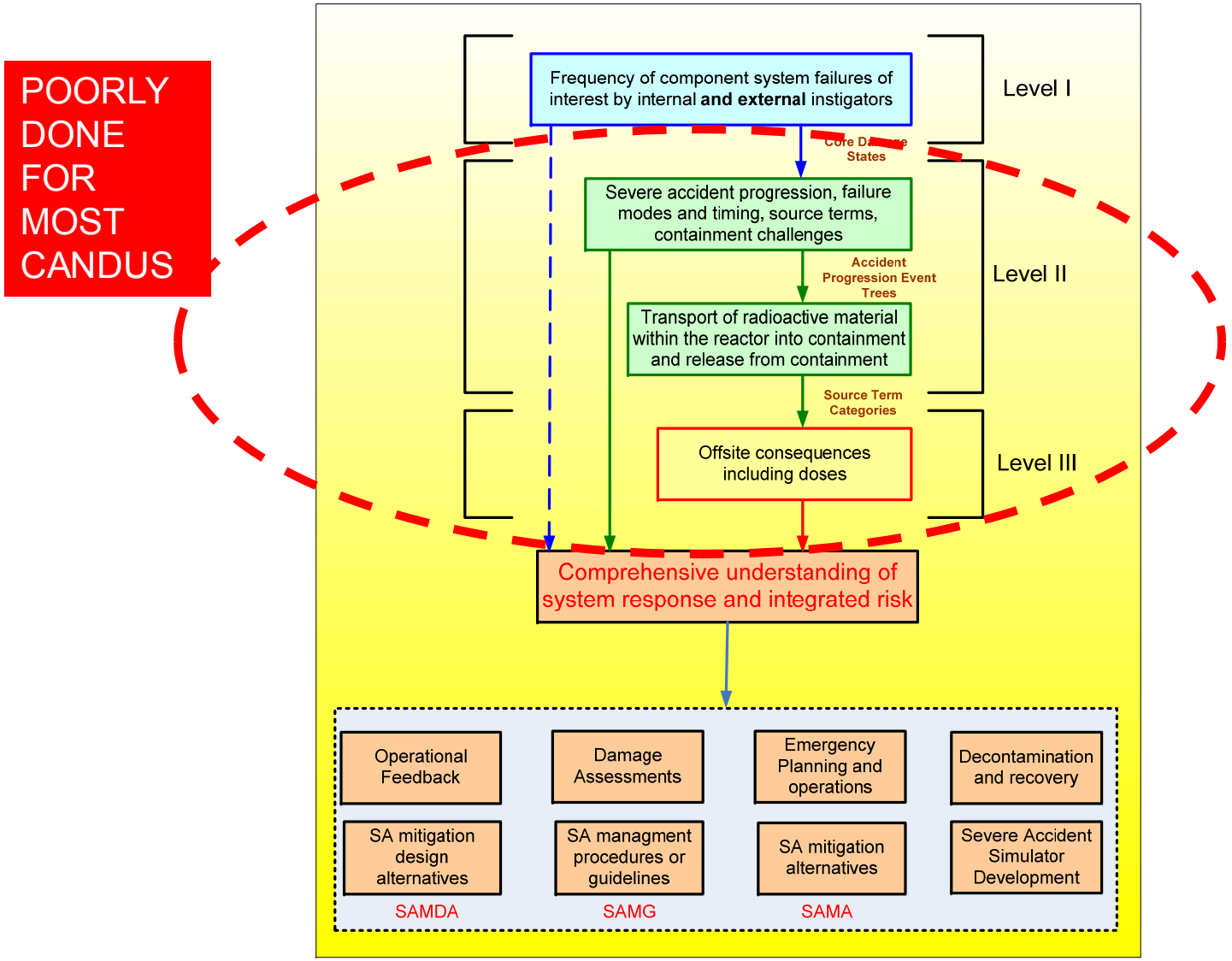


Figure 12 : RISK EVALUATION AND RISK REDUCTION PROCESSES

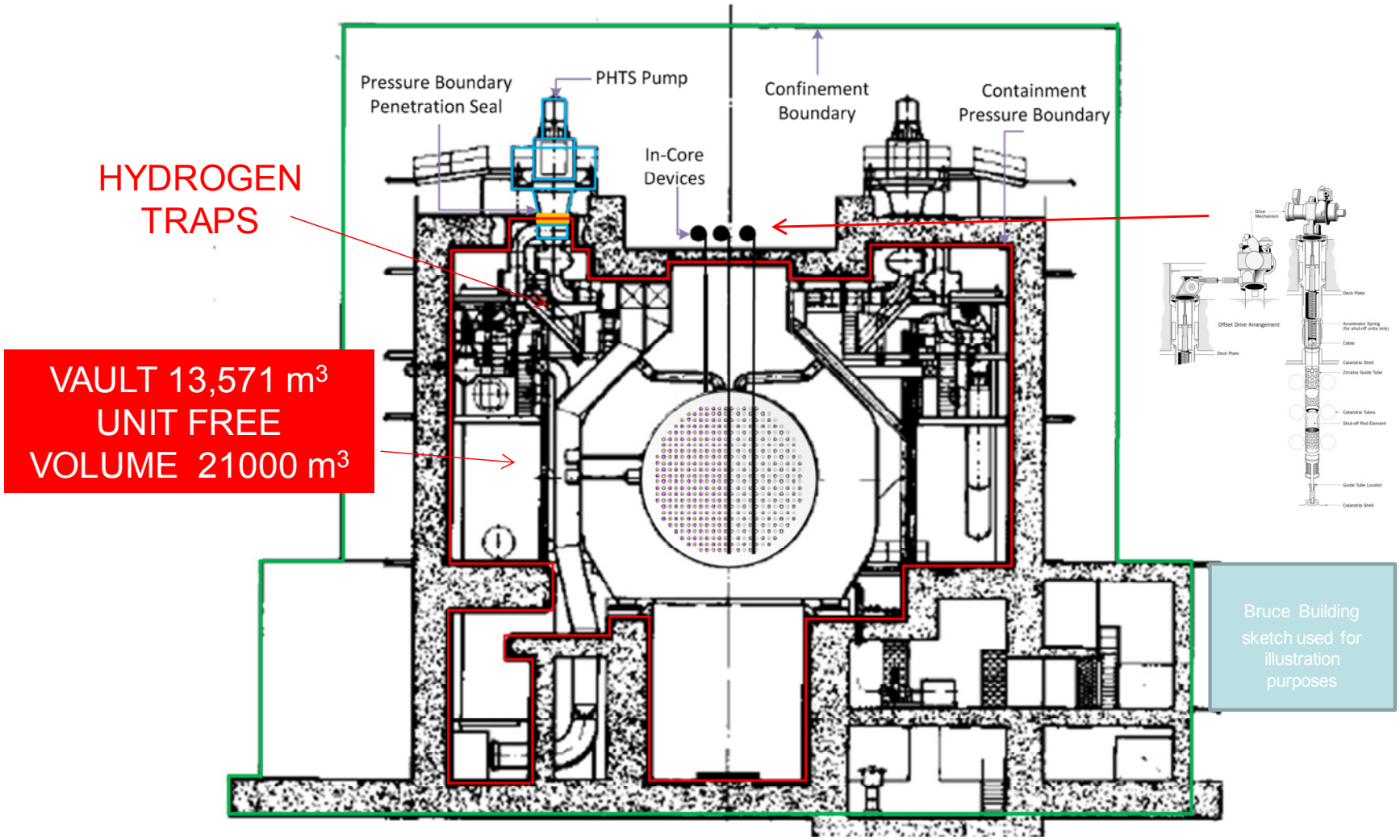


Figure 13: ISSUE OF HYDROGEN TRAPS IN DARLINGTON CONTAINMENT IN SEVERE ACCIDENTS

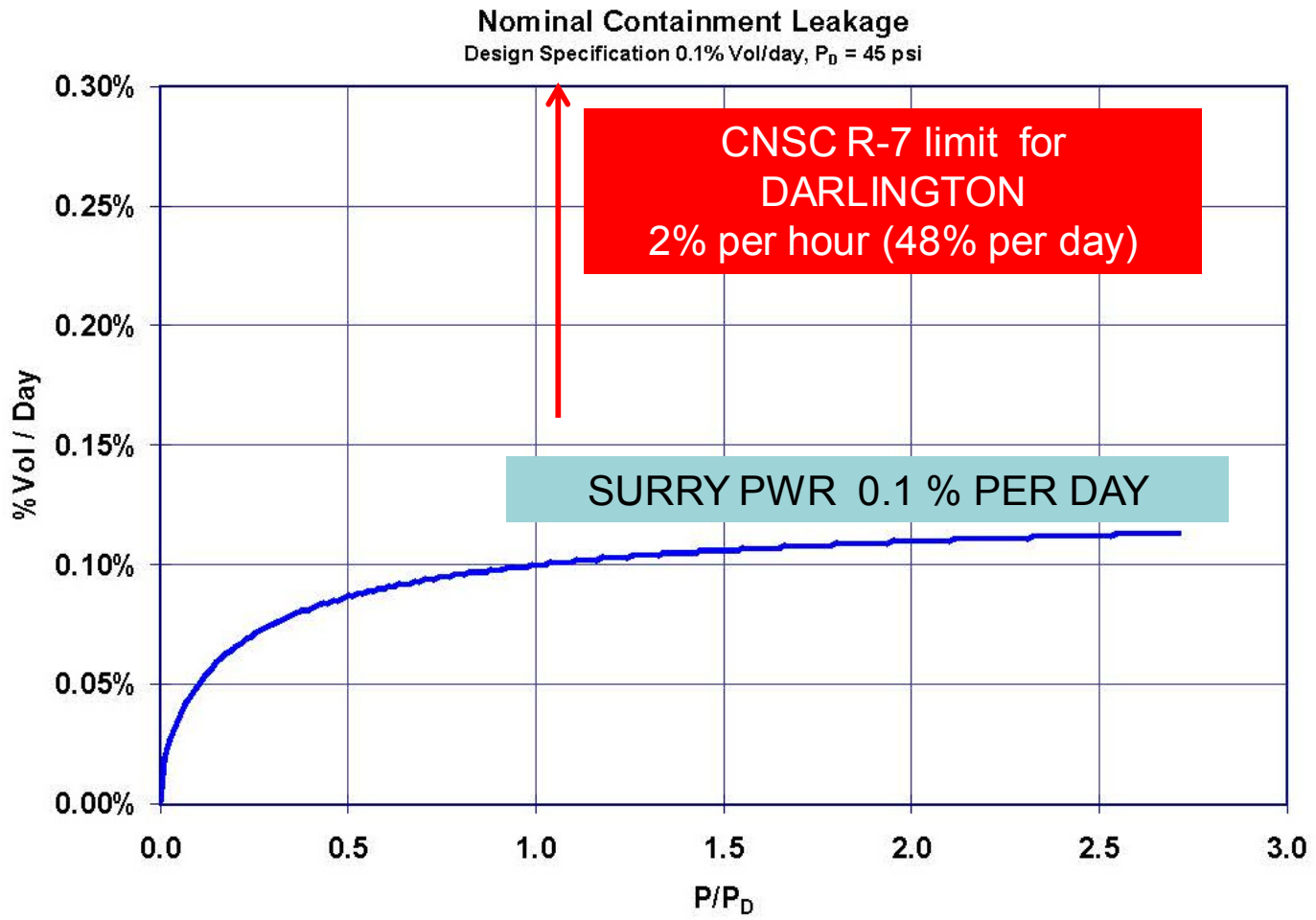
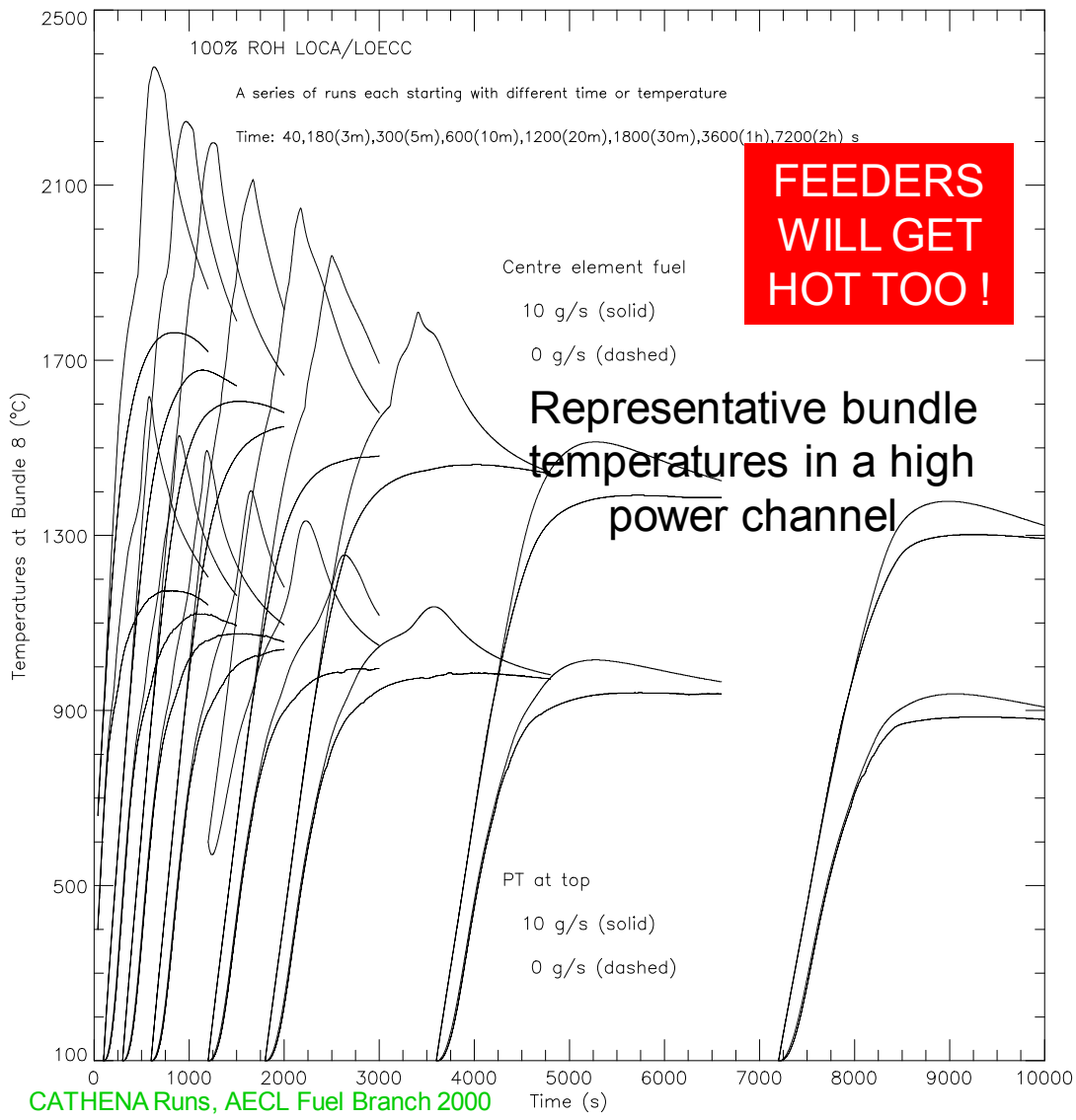


Figure 4-10 Nominal Containment Leakage Model Source : NUREG-7110

Figure 14: COMAPRISON OF PWR AND DARLINGTON CONTAINMENT ACCEPTABLE LAEKAGE RATES



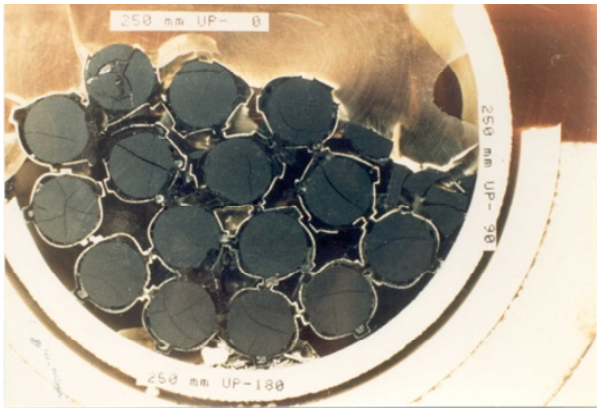


Figure 15 : Example of LOCA + LOECI fuel temperatures as a function of onset of fuel dryout

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

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

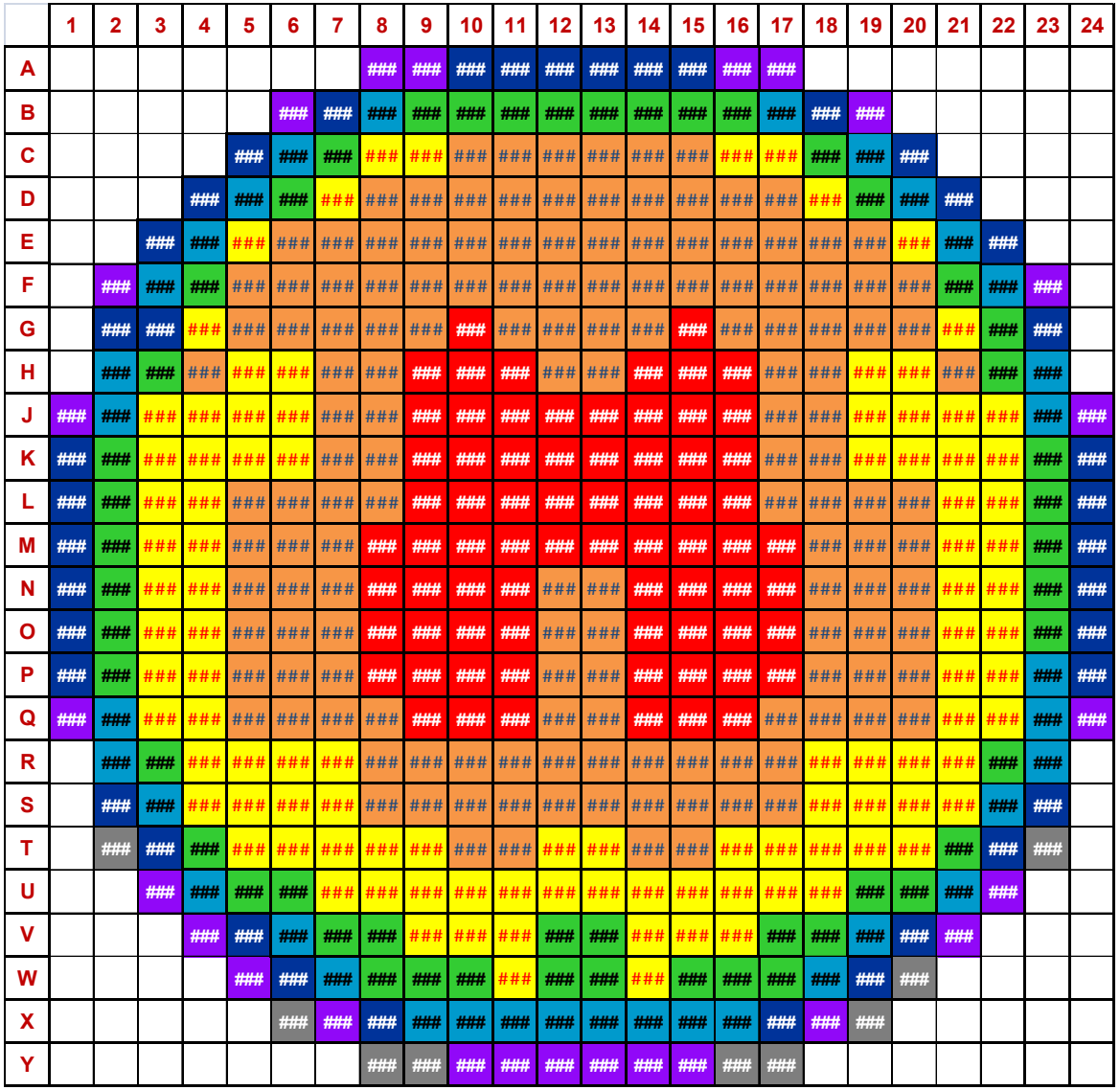


Figure 16: Channel Power ranges and feeders affect subsequent behaviour

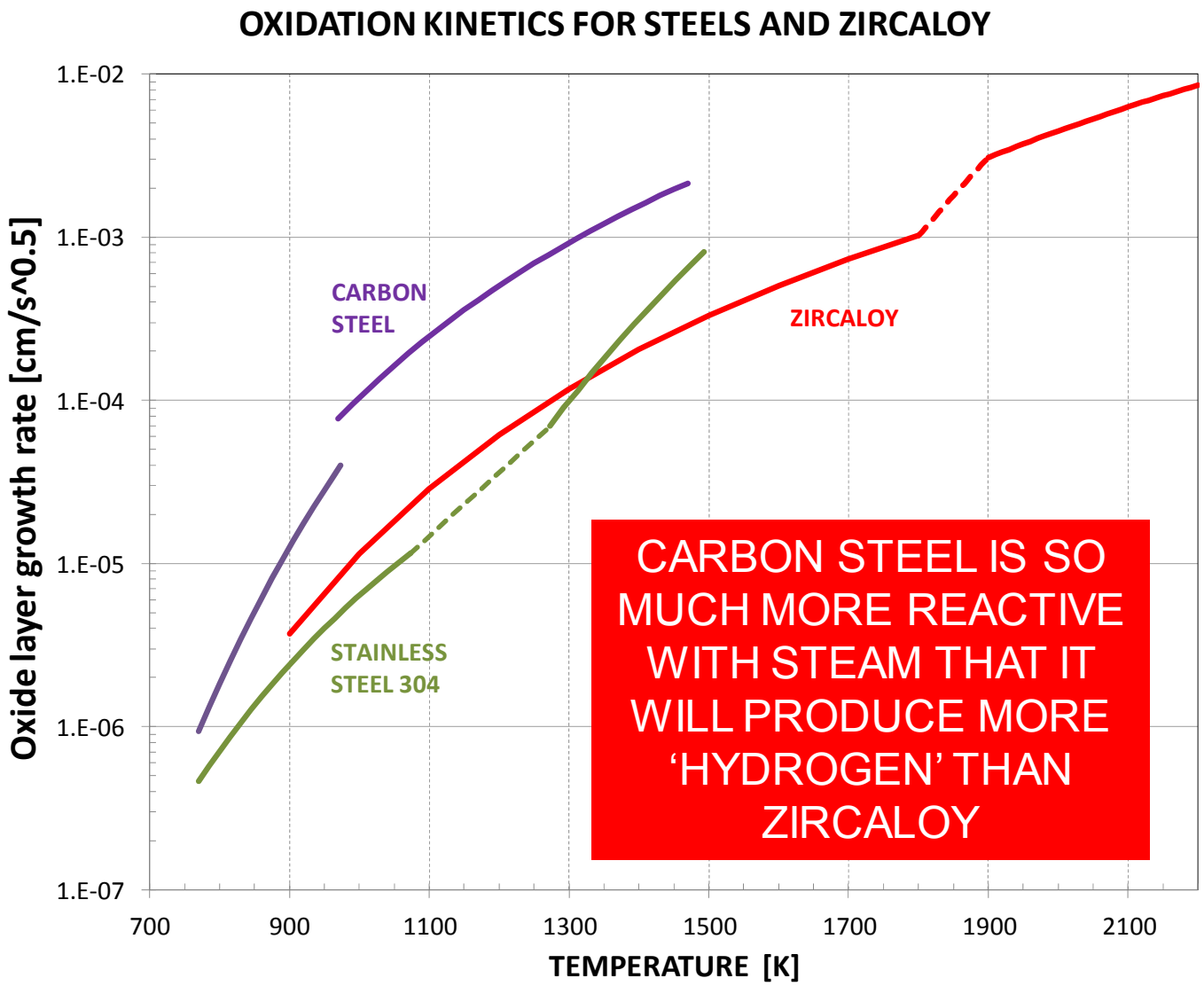
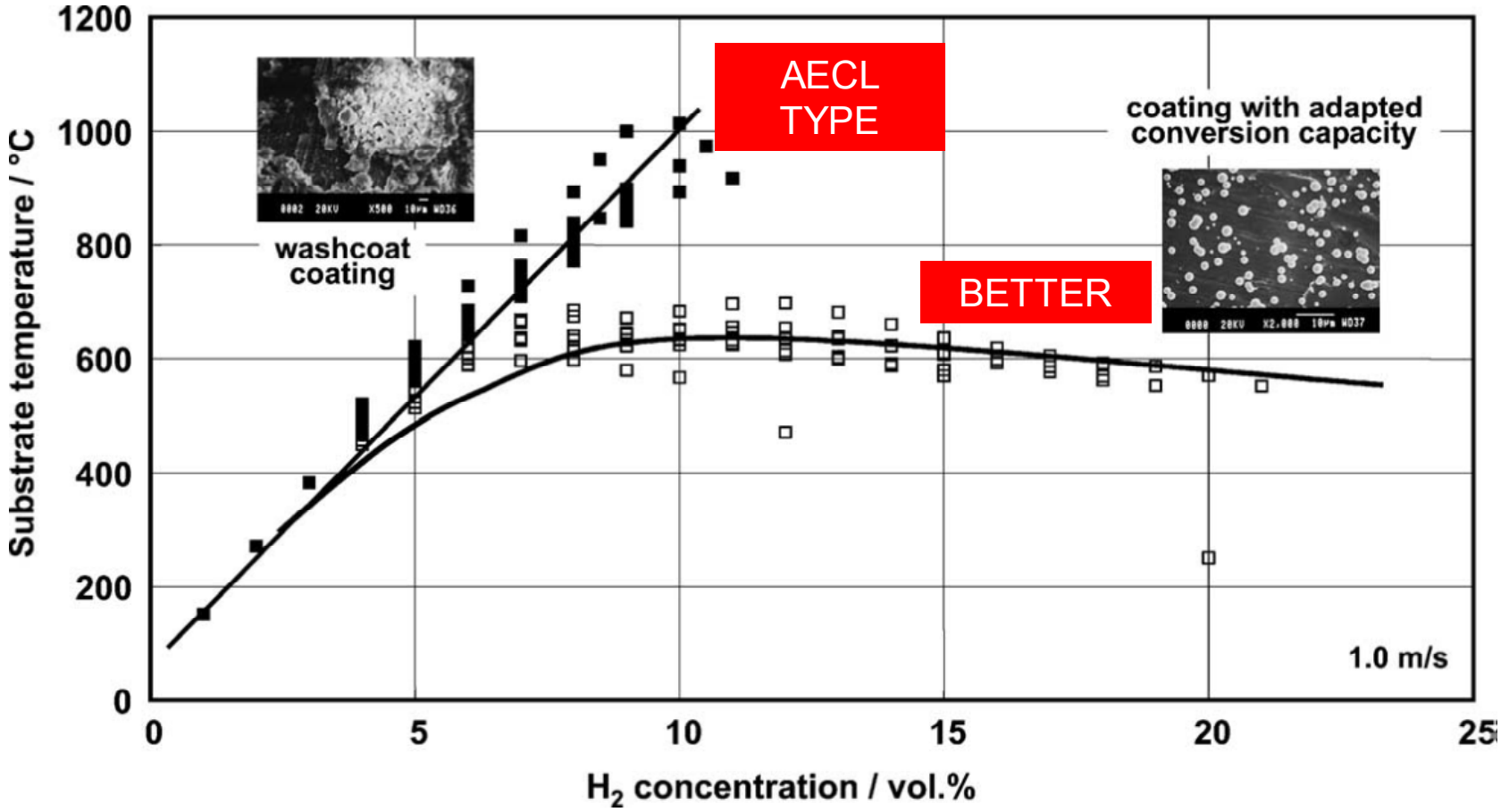


Figure 17 : Oxidation kinetics of different core materials



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

Figure 18: Typical PARS exit temperatures

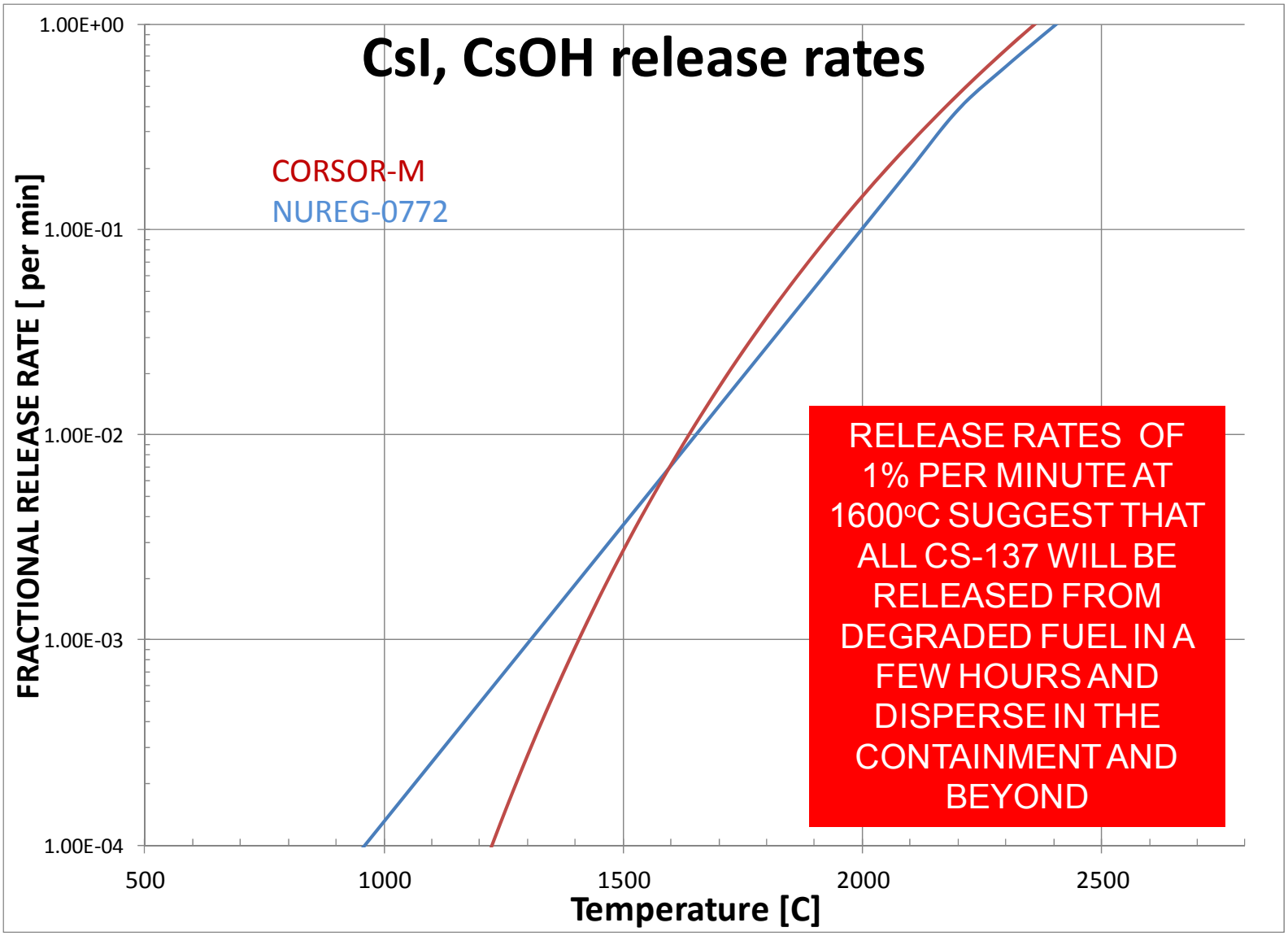


Figure 19: example of fission product release rates

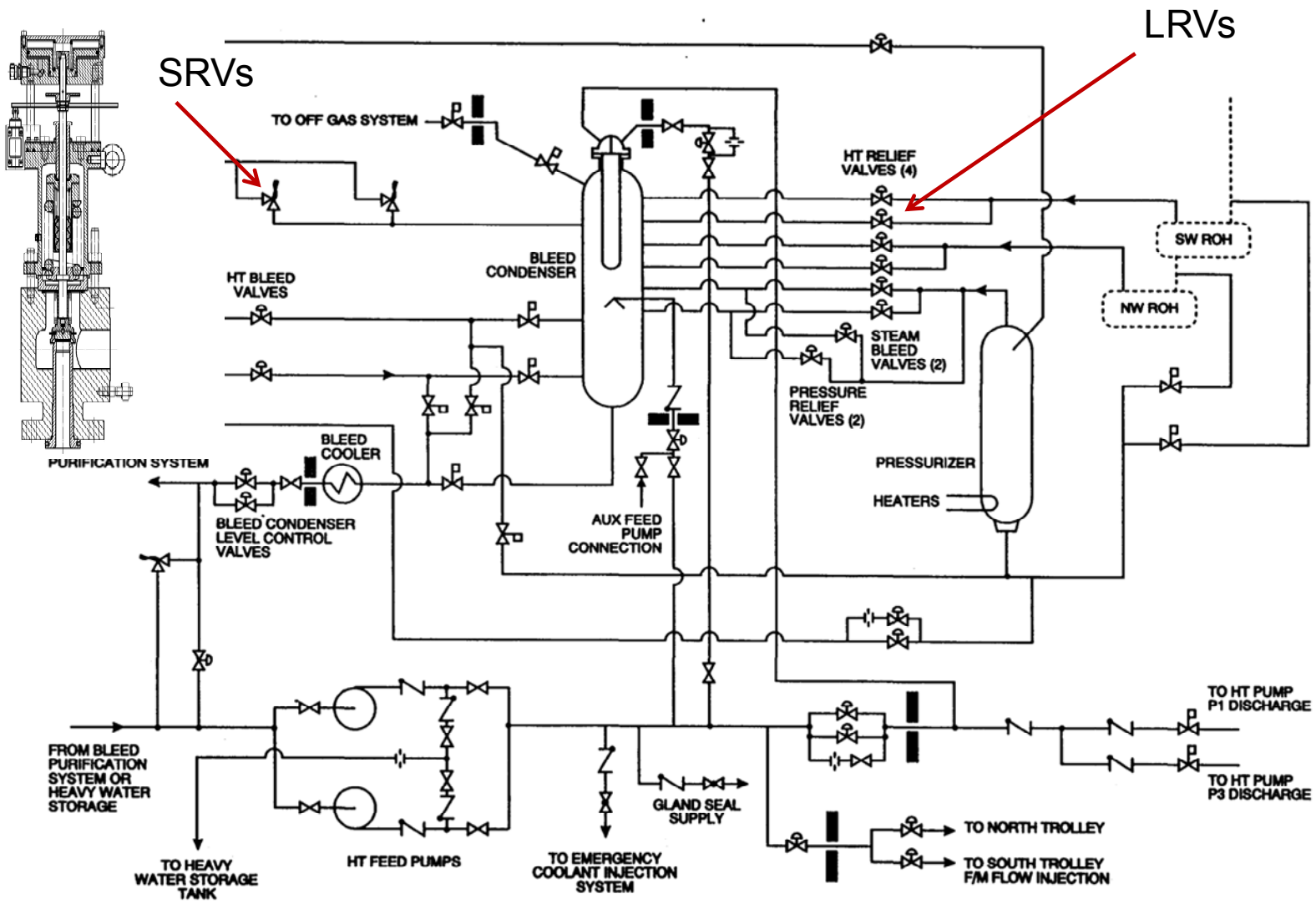


Figure 20: Darlington HTS over pressure protection - Left arrow shows SRVS, right arrow shows LRVs

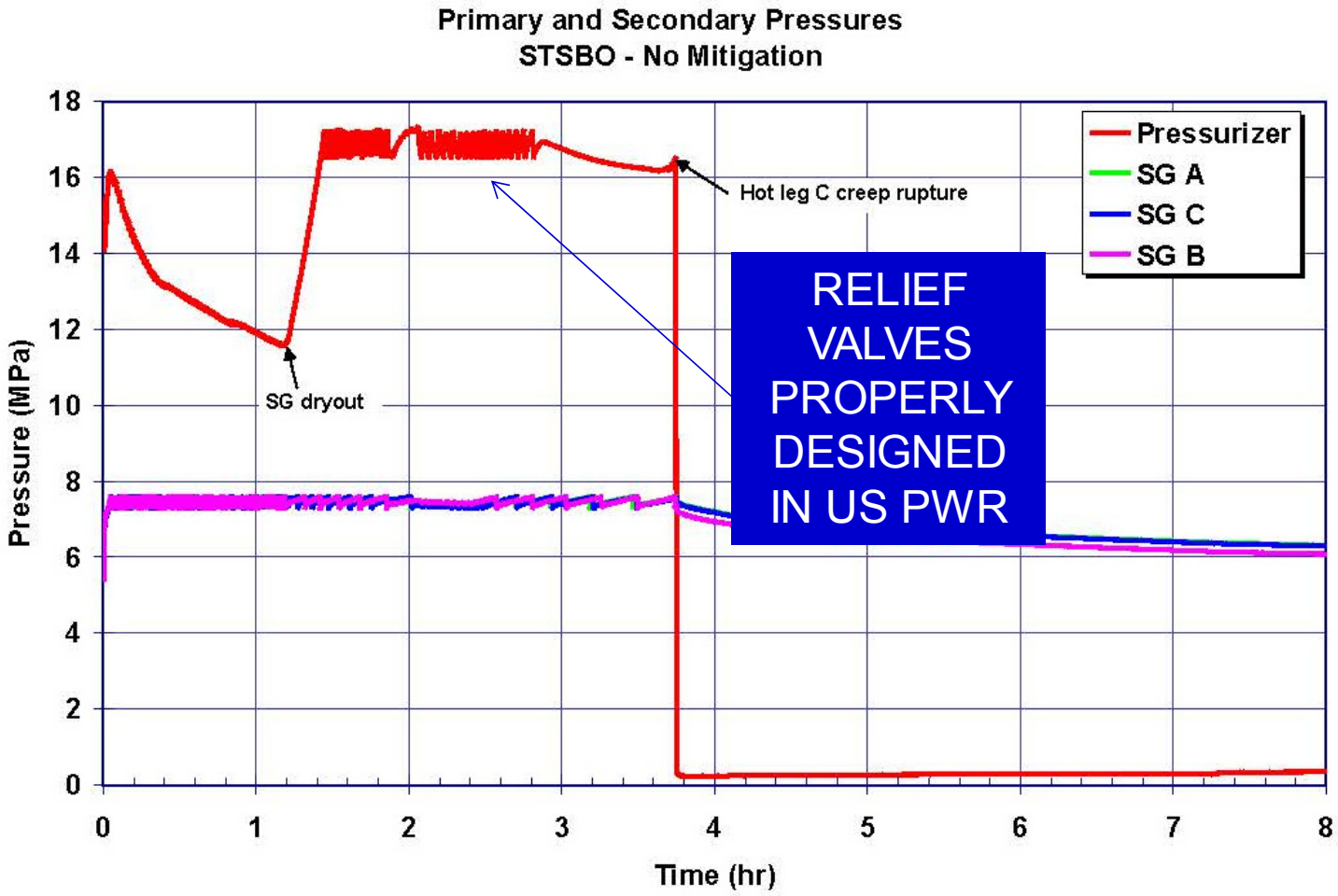
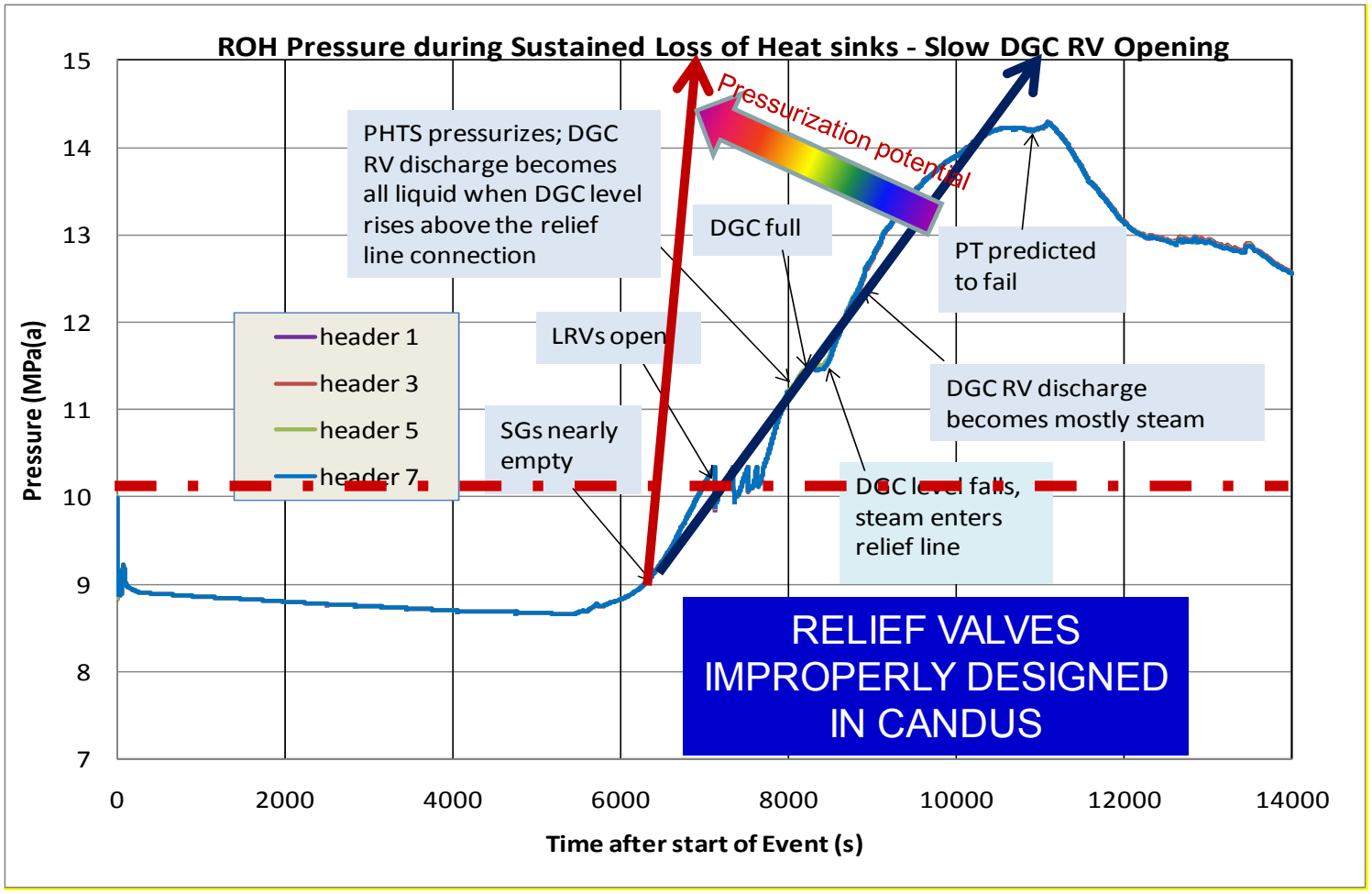


Figure 5-28 Unmitigated STSBO primary and secondary pressures history

Source – NUREG/CR 7110

Figure 21 : Example of PHTS response to a properly designed relief valve



Source : AECL 2011

Figure 22 : 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)

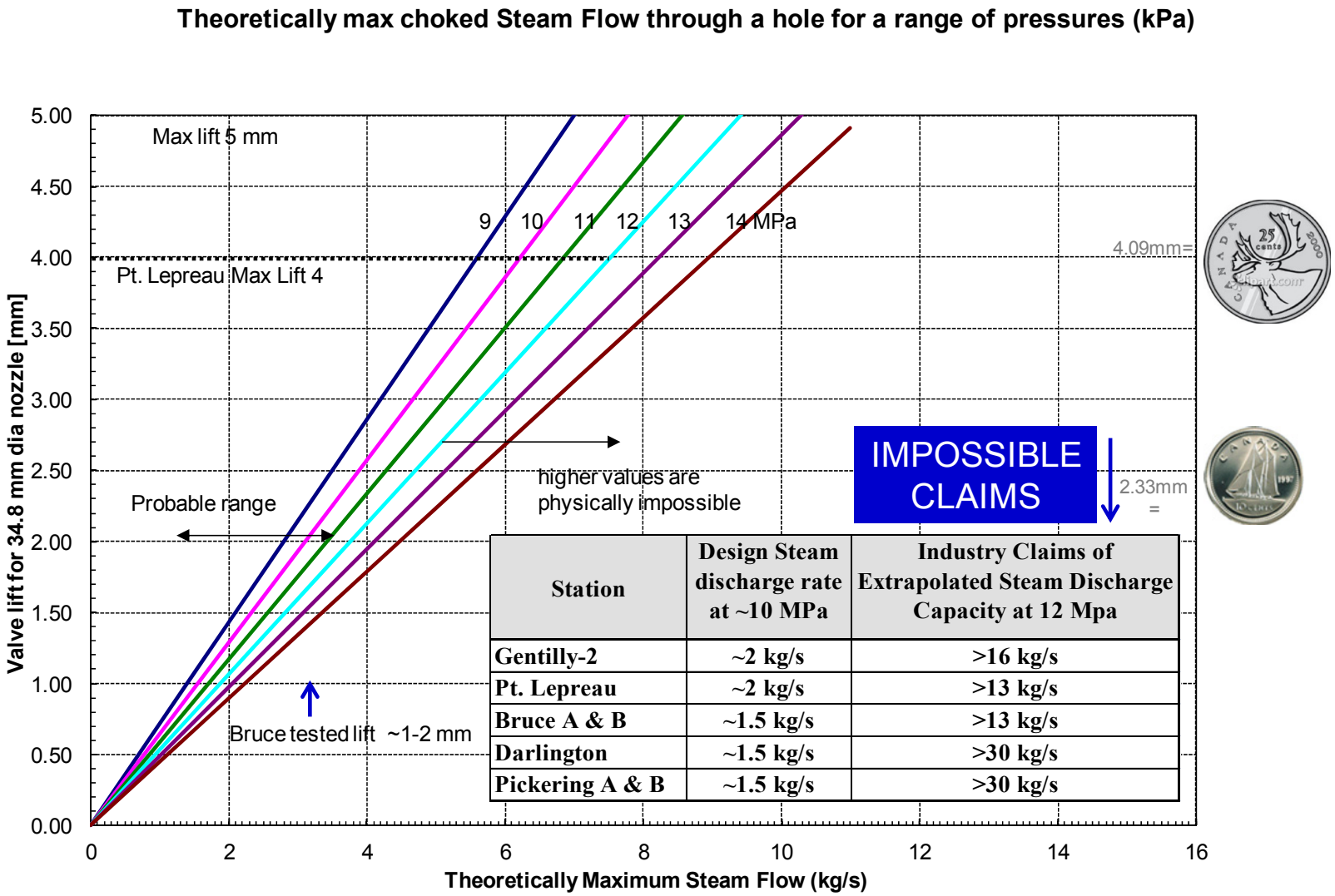


Figure 23: Sample calculations to demonstrate that Bruce safety relief valves with 1mm lift cannot relieve enough decay heat steam (~20 kg/s) to avoid an uncontrolled rupture

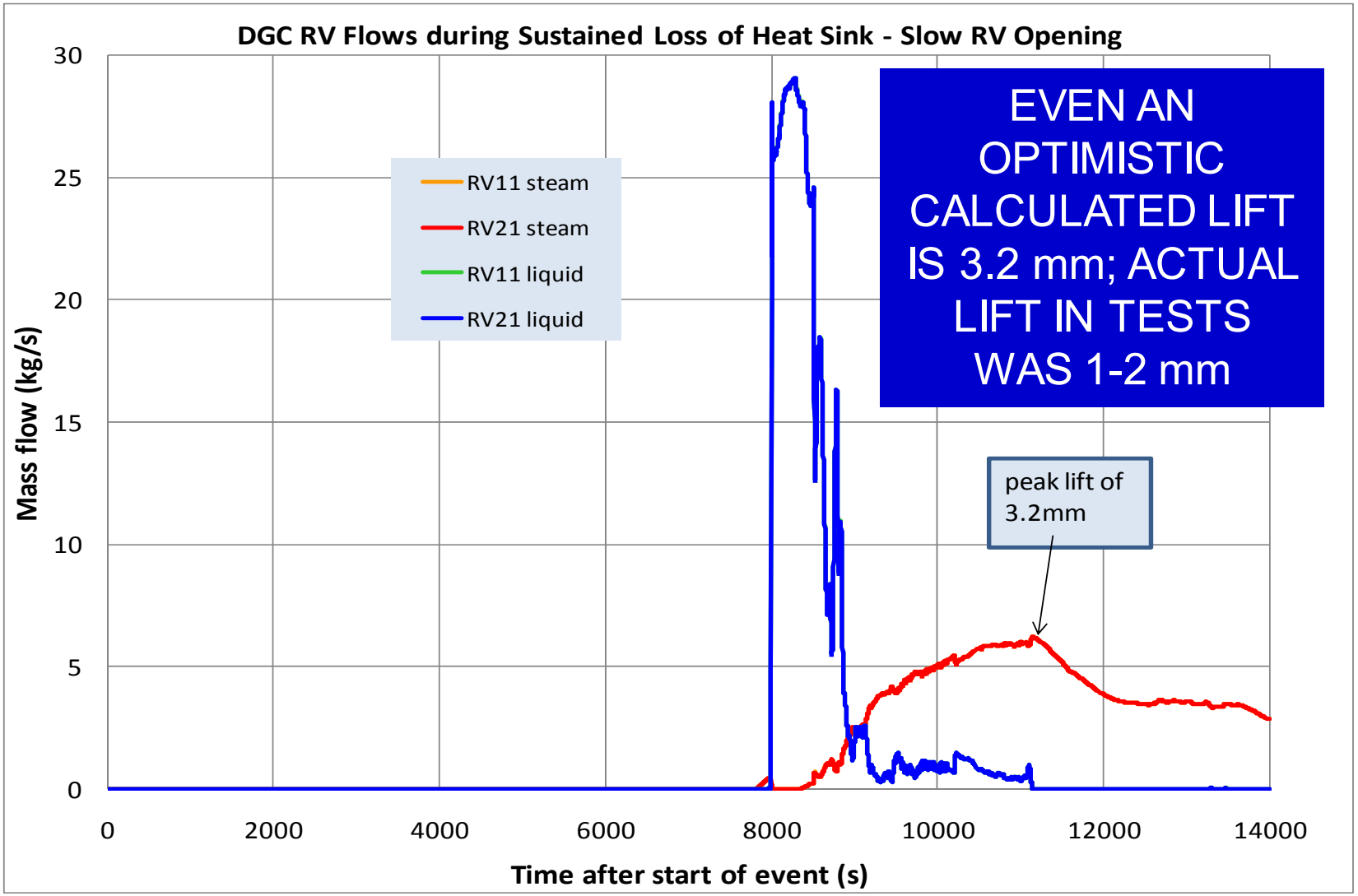


Figure 24 : AECL calculations confirming that the steam relief capacity of the Bruce type safety relief valves at <10 kg/s is inadequate and will cause uncontrolled ruptures

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.