Canadian Nuclear Industry Position on Proposals .vs. Actual Measures Undertaken to Reduce Severe Accident Risk from CANDU PHWRs

Sunil Nijhawan, PhD, P.Eng
Prolet Inc, Toronto, Canada
Sunil@Prolet.com

ABSTRACT

Nuclear power reactors are licensed and operated with an explicit public understanding and agreements between the stakeholders to continuously reduce the risk from their continued operation to public. Assurances of huge safety margins, organizational competence, low probabilities and benign consequences of any accidents are part of the licensing process to not only safeguard public interest but also reassure the public. Accidents that cause significant off-site consequences are written off as incredible. However, after two other unforgettable experiences attributed later to bad operator training and a poor design, Fukushima finally shattered the façade of incredibility of severe core damage accidents in power reactors. It also brought out into public discussions lapses in safety culture and the cozy relationship between the people who operate and regulate them. The actions of the regulators and utilities since Fukushima now put into question the façades of 'Safety First' and organizational competence and question their willingness to accept that these reactors are now obsolete and need to be either retired gracefully or seriously upgraded.

Twenty five years of comprehensive, independent, deterministic analyses of severe accident progression in CANDU reactors have unveiled a number of design specifics and reactor response pathways that indicate an unacceptable level of potential for risk to the owner utilities, motherland and public. These investigations have been conducted using multiple integrated computer codes and analytical methods developed by this author for system response to severe accident progression after a station blackout scenario for reactors and for certain design basis accidents.

In spite of ample evidence in support of the issues that have been raised at various forums and in various reports and licensing submissions, the reactor owners, operating utilities and Canadian regulator CNSC have decided to jointly ignore these and other similar findings and have continued operation without undertaking necessary and critical measures to reduce risk to the unsuspecting public. Lessons of Fukushima have remained unheeded.

INTRODUCTION

Probabilistic safety assessments document the initiating events and theoretical permutations of failures that can lead to a severe core damage. Common to all such accidents is the loss of primary and secondary heat sinks such that fuel decay heat cannot be removed and the fuel assemblies heatup, deform and crumble into rubble. A coincident loss of moderator as the secondary heat sink is a CANDU specific requirement for what is classified as a severe core damage accident, an event that is beyond the design basis and results from multiple failures. A design basis accident with an inability to quench the core with ECC after a LOCA that results in widespread fuel damage (even without moderator loss) is a very close second and also an issue of concern here.

In context of a simple to understand and widely plausible sustained loss of electrical power (station blackout) as at Fukushima, the CANDU reactor vulnerabilities that need to be rectified include those that cause early and uncontrolled primary coolant pressure boundary ruptures; premature expulsion of critical coolant from main coolant loops and from the moderator heat sink; direct exposure of overheating core debris and fission product releases to the containment; thermo-mechanical failure of the thin shell Calandria vessel welds; accelerated and excessive production of combustible Deuterium and Hydrogen; containment boundary failures from pressurizations caused by energetic interactions of fuel debris with water and by hydrogen explosions triggered by sparsely populated and ill-designed PARS units potentially exposed to high concentration of Deuterium / Hydrogen they are unable to adequately mitigate and thus overheat to

cause auto-ignition. This can result in unacceptable off-site radiological consequences in host communities that will make Fukushima consequences look like a walk in the park.

One recalls the conclusions of the investigations into the Fukushima disaster (references 1, 2) and wonders if the malaise of utility-regulator collusion and deterioration of safety culture is limited to just those countries and technologies that have already seen 3 severe accidents in less than 15,000 worldwide reactor years of operation. Documented evidence now shows a wide spread practice in Canada of the industry glorifying the 'inherent' CANDU safety features (*water all around* !!) and superior 'safety culture' with what effectively is minimal real public accountability with the regulator acting like a cheerleader and an industry proponent.

A number of properly engineered design enhancements can and must be undertaken to reduce risk from a severe accident by systematically identifying, eliminating, subduing or avoiding some of the undesirable system responses that the otherwise robust CANDU design challenges us under the beyond design permutations of failures that lead to severe core damage accidents. Additionally, innovative accident detection, control and mitigation measures and operator training can be put in place to avoid some of the undesirable accident progression paths to reduce the likelihood and consequences that these reactors can unexpectedly inflict.

This would have required starting with improved analysis of the underlying accident progression issues, an acceptance of basic engineering fact based evidence, an honest discussion and a cooperative effort by all stakeholders. Instead the industry (and that is not only exclusively in Canada) has decided that shouting down the bad news with hyperbole of CANDU superiority and their equally superior (*world leader !!*) management acumen is more expedient and profitable than fixing the underlying deficiencies in interest of public safety. Slogans *(we will never compromise safety !!*) have replaced hard engineering work. Certain reports (references 3, 4) and statements put out by the regulators with industry support amount to willful negligence of their legal responsibility to safeguard public safety in continued reactor operations.

There has been a lot of noise on the topic of improved severe accident mitigation but nothing really much has changed since Fukushima. More than five years ago, the Canadian regulatory body CNSC prepared a number of investigative requests (Fukushima *'Action Items*') as part of post Fukushima reviews but then quietly and surprisingly accepted measures and submissions that do not meet that intent or the public expectations for risk reduction from severe accidents after Fukushima. All Action items have long since closed without critical hardware upgrades. Even measures as fundamental as overpressure protection and combustible gas mitigation have been ignored, notwithstanding the weak and leaky containments in which most of Canadian CANDUs are housed with reactor cores that will release radioactivity directly to the containment without the benefit of a LWR like retaining pressure vessel that isolated the core debris and minimized TMI accident consequences. Bearers of bad news are vilified and unsuspecting local governments responsible for organizing off-site response are presented incredibly unrealistic and optimistic picture of off-site consequences they must prepare for. They are told in Ontario to prepare for no more than 0.15% of the total inventory of risk critical fission product species' releases from reactors. Reality of overheating and melting reactor core activity releases of ~1% per minute directly and without attenuation into weak and leaky containments is not discussed.

Without thoughtful and timely design changes, consequences of a severe core damage in a single unit CANDU-600 MWe reactor (Wolsong, Embalse, Pt. Lepreau, Cernavoda, Qinshan) can cause off-site damage that are unacceptable and surprising; especially after the hype that surrounded the European utility ‘Stress Tests’ and Canadian regulatory ‘Action Items’ that dutifully appeared and disappeared following Fukushima disaster in 2011.

Other, multi-unit CANDU reactors (Bruce, Darlington, Pickering) are worse off and sport higher risk profiles due to their very weak and very leaky containment structures and pressurizers that are located below the core (Bruce, Darlington) thus potentially sucking up primary coolant from the boilers and inhibiting success of actions to

restore boiler heat sinks. A dozen other vulnerabilities, including low elevation and first to lakeshore placements of backup diesel generators (as in Fukushima) make the potential consequences worse. This has not stopped the regulators from granting them 10 year licenses.

This paper lists a series of proposals that were made in interest of risk reduction and summarizes in a few words the disappointing and irresponsible position taken by the Canadian CANDU utilities to avoid dedicating resources required for implementing comprehensive severe accident related design improvements and putting in effective mitigation measures consistent with the actual design. References 5 , 6, 7 discuss many of the issues and potential solutions in further detail.

There also have been critical, pre-meditated, well orchestrated, mis-information measures (references 3, 4 and transcripts of public hearings for Darlington (2015), Bruce (2015,2018) and Pickering (2018) reactors hopefully still available at CNSC website) by the collusive and compliant national regular CNSC such that information provided to the local governments is blatantly misleading and will lead to un-necessary fatalities including that of first responders, untold economic damage and disruptions, especially if the emergency response actions are based on that faulty and deliberately misleading information. Some concerns about regulatory behaviour are summarized in reference 8.

As we discuss the underlying technical issues, summarize specific responses and actions by the industry and regulatory staff and paucity of their arguments to the contrary, it is hoped that information (and references 5, 6 and 7) will help Korean utilities dedicate required resources to necessary improvements and public pressure will guide the regulators in shutting down the plants in absence of necessary and responsible response by the licensees. It is also mildly hoped that a revamped, new regulatory regime in Canada will provide the necessary leadership as well.

ENHANCED SEVERE ACCIDENT RISK

There is no question that any of the currently operating CANDU reactors, designed 40-50 years ago, will not be allowed to be built today in any jurisdiction that has built a responsive, accountable, law abiding, rule based, robust regulatory regime. As built, these reactors just do not meet the current public expectations of risk profiles against initiating events that lead to severe core damage accidents. Severe accidents were not within the design basis of any of the operating reactors of any pedigree or design - and can only be mitigated with improvements in design and other measures or gracefully retired as it started in CANDU industry with Gentilly-2 and Wolsong-1 reactors and with scores of LWRs in many countries.

For CANDUs certain severe core damage accidents that fall under the licensing basis - such as LOCA+LOECC (Loss of coolant accident with a coincident Loss of Emergency Core Coolant injection) are also poorly considered in safety assessments and poorly mitigated. For one, the Deuterium source term is grossly underestimated and the ability of available hydrogen mitigation measures to avoid explosions is highly questionable. As a result off-site consequences can go off the chart very quickly.

In order to put the design improvement suggestions in perspective, let us first look at response of a single unit CANDU-6 (say at Wolsong) PHWR to a simple station blackout. After a sustained loss of AC power, an approximately 60% boiler inventory depletion leads to an unusual for a nuclear power reactor, over-pressurization of the Heat Transport System due to a grossly undersized primary safety pressure relief. An uncontrolled failure of a pressure boundary component in the main core cooling circuit, likely to be boiler tubes, results in a potential containment bypass and early population exposure to fission and activation products. A serious re-design error (introduced spuriously in 1996 after a safety relief valve at a Pickering CANDU stuck open) in HTS pressure relief capability creates a containment bypass path for off-site contamination well before there is any severe core damage. So a benign outcome that can be terminated by ECC, transforms into a serious uncontrolled rupture accident whose economic consequences can be significant even if a subsequent coolant injection by ECC is successful. Recall that an uncontrolled over-pressure failure is basis for likely never being allowed to put the

reactor back in operation. A failure to undertake a $38k valve upgrade results in a multi billion dollar loss in any event, whether leading to a severe core damage or not. See reference 9 for more details.

With boilers no longer a heat sink (from about 1.5 hours), downward progressive onset of fuel channel voiding and dry fuel bundle heatup leads to a partial voiding of the Calandria vessel. In absence of a suitable relief valve on this vessel, the four large rupture disks cause an un-necessary moderator flashing / carryover expulsion upon onset of moderator boiling. Conditions for severe accelerated core damage are created by a simple design omission.

With some high elevation fuel channels thus immediately losing all heat sinks, conditions form for accelerated fuel channel overheating, fuel deformations, bundle dissociation and core disassembly at about 5 hours. At an average temperature of ~1500^{o}C about 1%/min of activity inventory of long lived and risk dominant species such as Cs-137 are now dumped into the containment with each channel uncovery. With no pressure vessel to completely isolate the overheating fuel from the containment, the fuel & suspended channel debris heatup to release fission products fast.

Uncovery of additional, lower lying channels over next few hours results in a direct expulsion of un-attenuated fission products into the containment which has a relatively low failure threshold at penetrations and airlocks. Given the large amount of Zircaloy (>43 tons) in reactor channels and low chromium carbon steel in the CANDU feeder pipes (>8km long, ~1800 m^2 surface area to oxidize internally by steam and externally by air each), accelerated Deutrium gas releases into the containment readily exceed the detonation limits as the small number of poorly designed Palladium compound coated passive recombiners are not only unable to arrest the increase of deuterium concentration but also introduce ignition surfaces leading to destructive combustible gas detonation. Early breech of the containment pressure boundary by simple overpressure of just above 1.24 atm(g) at airlocks is also unavoidable.

The terminal debris formation in a CANDU reactor is largely in solid chunks of channel segments and fortunately occurs over a about a day although the fuel failures and releases into the containment of fission products from within the intact channels is relatively fast. The eventual retention of debris upon melting (as in a PWR vessel) in the Calandria vessel cannot be guaranteed as the relatively thin walled stepped and welded vessel (wall thickness varying between 19 and 28 mm - designed to hold just cold water at low pressures) may easily fail at welds thus introducing water from the shield tank (reactor vault) onto the hot dry debris. The effect of these weld failures would depend upon the break area and rate of water ingress onto hot, dry debris that caused thermal stresses in the stepped welded vessel to initiate weld failures. It can vary from additional exothermic oxidation, additional hydrogen production and accelerated fission product releases to violent vessel and structure failures by energetic and mechanically violent interactions of shield tank water with remaining hot and solid-liquid debris at the bottom of the vessel.

Significant and almost total releases of fission products into the leaky containments cannot be precluded as all potential accident mitigation pathways are convoluted. For example, if the early uncontrolled over-pressurization caused failure of a channel that ejected its end fitting and drained the moderator, no recovery actions will work well enough to arrest fission product releases. Early termination of accident is also complicated by an inability to manually depressurize the heat transport system directly and add coolant to it at high pressures. An absence of high pressure injection mitigation systems for either of the primary and secondary cooling circuits will cause invocation of ill-conceived emergency measures that can in reality accelerate core damage (like boiler depressurization to use the deaerator or emergency boiler water inventory; thwarted by check valve 'cracking pressure'). One more reliable solution for restoration of feedwater is to have a steam driven turbine that does not require boiler depressurization. While scores of PWRs use this mitigation measures our regulators do not understand its merit.

Most CANDUs in Canada are in multi unit configurations. With a containment design pressure of well under one atmosphere and leak rate at design pressure of 2% / hour (480 times that

of a typical PWR with a 0.1%/day leak rate), there is also no question that the CANDU multi-unit reactors at Darlington and Bruce sport some of the weakest and leakiest containments of any reactor in the world. The reactor vessel placement at high points of the 4 unit interconnected containments will also cause trapping of large quantities of explosive Deuterium potentially produced by large amounts of Zircaloy and kilometers of cheap, low chromium, carbon steel feeder piping to fuel channels. A number of critical equipment like boilers and reactivity deck are outside the containment; something that is unheard of in other PWRs. They also have no pressure vessels to isolate from containment any overheating core materials. So the fission products released from overheating fuel will be ejected directly into these leaky containment structures built like rectangular industrial buildings and not classical cylindrical-spherical pressure retaining geometries of nuclear reactor containments around the world.

In absence of their engineered heat sinks, these reactor designs cannot remove full decay heat from any of the enveloping water volumes that by turn become heat sinks - Heat Transport System, Moderator System or the Shield Tank - without bursting them or some rupturing fuse disks to create a large path for fission products and fluid inventory ejected out. There also are again no means to directly depressurize the HTS or to add high pressure emergency coolant to it without an indirect and unreliable depressurization of boilers. The reactors do not have any meaningful Deuterium mitigation systems or core instrumentation to follow accident progression. There are no severe accident simulators and the table-top/paper SAMG exercises based on obsolete codes and rosy assumptions (e.g. of automatic gravity feed into boilers) are meaningless. The actual list of design weaknesses is significantly higher and certain measures to reduce risk from them are listed below.

The purpose of presenting this paper at KNS is to one final time warn the Korean nuclear stakeholders of the perils of a similar approach towards Wolsong CANDU station risk assessments and to draw attention of / to those who have failed to act on the available information on enhanced severe core damage risk so far.

AVENUES FOR RISK REDUCTION

The following list of generic CANDU severe accident related design and mitigation measure improvements were proposed :

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; de-aerator 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 in-core devices*
    - *More appropriate modelling by using D2O 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 D_2 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 a 100% 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*

INDUSTRY POSITION

In 2016 the CANDU Owner's Group (COG) published an industry supported report (Reference 10) on the above safety improvement suggestions. To celebrate its release, the CNSC held a meeting on March 8, 2017 on the same topic, invited external consultants; branded intervener as 'outlier' and 'intemperate' and hastily concluded, as expected, that none of the above proposals deserved further considerations.

Overall, all proposals were rejected by COG, including many that even an uneducated person on the street can easily relate to and will shake his/her head in disbelief. There are three possible explanations:

1) The proposals were not technically sound.
2) The COG and CNSC reviews were undertaken incompetently and/or in bad faith.

3) The present risk profile of the CANDU PHWR reactors is acceptable and no design changes or risk reduction measures are warranted.

This presentation will discuss the absence of any technical merits in that response and why it is indicative of a TEPCO-NISA like decline in safety culture that may precipitate an accident - severe or otherwise - at a CANDU plant that will cause the demise of an industry that so many of us have spent our life nurturing.

CONCLUSIONS

No country can afford any more the risk of a nuclear reactor severe core damage accident. It is more than 7 years after Fukushima today and all efforts should have been made to reduce the likelihood and consequences of such accidents by now. It is unacceptable and deplorable that this has not happened in the PHWR CANDU industry.

The three core damage accidents in less than 15,000 reactor years of operation and the resulting disruption of thousands of human lives and a near trillion dollar economic impact is an unacceptable outcome for an industrial activity solely geared towards selling electricity for a few decades. Since this happened in three of the most technologically advanced countries in the world and in all cases a very poor safety culture was also to blame, an immediate re-examination of severe accident vulnerabilities of CANDU PHWRs was undertaken by us and issues thus uncovered were raised publically. Our 30 years of experience in modeling CANDU severe accidents put us in a unique position to do so.

The intransigence of the industry has been emboldened to insolent resistance to any change as an insistent inbred coupling and collusion between the utilities and the regulators has led to their summary rejection of any and all suggestions for improvements in CANDU reactors in Canada.

Perhaps reactors at all CANDU stations need to be shutdown pending independent public examination of the associated severe accident related risks. Role of all stakeholders, especially that of senior management at CANDU utilities and regulators should be publically investigated before an avoidable severe core damage accident consumes another country's economy and public peace.

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

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

5 Challenges in multi-unit CANDU reactor severe accident mitigation strategies, ICONE24-60689, Proceedings of the 24th International Conference on Nuclear Engineering ICONE24, June 26-30, 2016, Charlotte, NC, USA

6 Conversations About Challenges In Multi-Unit CANDU Reactor Severe Accident Mitigation Strategies, N11P0543, NUTHOS-11: The 11th International Topical Meeting on Nuclear Reactor Thermal Hydraulics, Operation and Safety, Gyeongju, Korea, October 9-13, 2016.

7 Opportunities And Need To Further Upgrade CANDU Reactors For Improved Severe Accident Mitigation And Reduction Of Risk, ICONE23-1053, Proceedings of ICONE-23, 23rd International Conference on Nuclear Engineering May 17-21, 2015, Chiba, Japan

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

9 Importance Of Reactor Heat Transport System Overpressure Protection System Under Severe Accident Conditions With Special Reference To CANDU Reactors, Paper 54301 , Proceedings of the 20th International Conference on Nuclear Engineering, ICONE20 & POWER2012, July 30-August 3, 2012, Anaheim, CA, USA

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