POWER REACTOR SAFETY COMPARISON – A LIMITED REVIEW

D.A. Meneley[1] and A.P. Muzumdar[2]
[1]University of Ontario Institute of Technology
[2] CANDU Owners Group

Abstract

A large amount of attention has been paid to avoiding positive coolant void reactivity in LWR reactors. This can be justified due to specific accident events that could lead to severe consequences. Somewhat less attention has been paid to other accident sequences that can lead to positive reactivity addition. Other designs, for example the CANDU-PHWR, exhibit positive coolant void reactivity but include both inherent and engineered systems that compensate for this undesirable characteristic. This paper represents the beginning of a long-term process intended to enable a balanced and fair comparison of the real safety of all reactor types.

1. Introduction

The formal report that led to the production of this paper was issued for public distribution in 2009 [1]. This paper highlights only two of the several points brought forward in that report; a companion paper in this conference examines some other aspects of the report's findings.

This paper has two objectives. The first is to place the Postulated Initiating Event (PIE) [2] identified as Large Loss-of-Coolant into proper context with similar accident events in both pressurized water reactors and boiling water reactors. The second objective is to initiate a logical process for inter-comparison of the safety of various reactor types, within the context of the International Convention on Nuclear Safety [3].

There are many possible definitions of a "safe" reactor. For reactors employing solid oxide fuel, the most elementary demonstration of safety is the one in which it can be proven that all (or almost all) fission products remain within the fuel sheath following all PIE. Implicit in this requirement is that the fuel pellets should never reach the molten state. Additional limits are placed on fuel enthalpy if the energy is added very rapidly. Of course, this condition – sufficient fuel cooling -- must be maintained in the long term following any accident.

In the early days of uranium energy utilization there was no need for comparison of safety on an absolute basis. Regulation was purely a national matter, and local judgments of sufficient safety were independent of one another. This situation has changed. Several different reactor concepts are, or soon will become, part of the generation mix in the world. Naturally there is a tendency for each commercially-driven entity to claim that the plant they build is "safer" than its competitors' products. There is still no common yardstick by which safety can be measured.

This Convention on Nuclear Safety was adopted in 1994 with the objective of normalizing and "equalizing" in some fashion the safety requirements of various nations. Its aim is to legally commit participating States operating land-based nuclear power plants to maintain a high level of

safety by setting international benchmarks to which States would subscribe. Four review meetings have been held. However, there is still no agreed means for comparing the absolute risk from operation of one power plant type with the operating risk of any other nuclear plant.

Probabilistic risk analysis is sometimes considered for safety inter-comparison. This method is extremely valuable in most situations, especially for judging the relative reliability of plant components and systems within a single plant design. The method is limited, however, in some very important aspects. The first is the question of completeness; that is, the question as to whether or not all important postulated initiating events (PIE) have been considered. The second limitation arises from the nature of some accident sequences. Such sequences may lead (as they have in past accidents) to extreme-value consequences, even at a relatively high frequency of occurrence. This situation arises because of the basic fact of operation of nuclear plants they are complex systems operated by humans.

Safe operation of any nuclear station depends most heavily on the performance of the operating staff. At the same time, even a high skilled group of operators (e.g. the space shuttle team) can, through errors of commission and omission, induce system failures in so many different ways and combinations that construction of a comprehensive model of the process is not practical.

2. Reactivity-Initiated Accidents

Reactivity-initiated accidents (RIA) have the largest potential for leading to large radioactive material releases because of their potential for adding reactivity up to and beyond the value of the delayed-neutron fraction, with consequent rapid energy addition. If the fuel of a solid-fueled reactor approaches or exceeds its molten state, most fission products are released and have the potential for causing damage at a distance.

With the exception of the CANDU design, RIA events happen too quickly to be controlled by engineered shutdown systems. As a result, many reactor designs must depend on the inherent mechanism of Doppler resonance broadening with increasing fuel enthalpy, to achieve timely reversal of the increasing total reactivity. The Doppler feedback phenomenon is very effective in this role, with one important reservation – the negative reactivity introduced by Doppler feedback must eventually be fully compensated by other systems (generally, engineered systems) before the reactor can be “rendered safe” [2].

This scope of this study was too limited to provide for complete analysis of even one RIA event in a power reactor, much less to carry out a comparative analysis of several cases. Even the presentation of results for one event is far beyond the space limitation of this paper. The approach taken in this work was to examine only the first few seconds of the event -- during the RIA power pulse -- and to examine the fuel enthalpy and total reactivity conditions during this time. Furthermore, the power pulses examined were taken from earlier analyses by others, mostly in the context of power reactor licensing applications.

The rationale for beginning the comparison of relative safety of different reactor types with this particular parameter is the fact that essentially all of the dangerous radioisotopes are normally

trapped in the fuel pellet, coupled with the fact that the pellet is the innermost effective barrier in the defence in depth design concept.

Tests of uranium dioxide fuel elements provide a quantitative measure of two important parameters. First, they indicate the maximum incremental enthalpy insertion to a fuel pellet prior to partial melting. The second useful item of information is the limit on rate and quantity of energy addition prior to fuel fragmentation. Subsequent analysis of RIA events can use these data as indicators of the onset of major release of fission products.

The prompt critical transition in a reactor with substantial negative reactivity feedback from Doppler resonance broadening determines the maximum total reactivity that will be reached in a transient because the negative feedback (proportional to the energy integral) is usually faster than the original positive reactivity addition rate. There is, of course, a limit to total Doppler feedback because fuel enthalpy limits are quickly reached in these cases. While the CANDU reactor has only a small negative Doppler coefficient, the rate of increase of reactor power is limited by its relatively long prompt neutron lifetime (about 40 times longer than that in a PWR). As a result the enthalpy rise rate is much slower in this reactor in the prompt critical range. It is slow enough, in fact, that engineered shutdown mechanisms become practical means for reducing the total reactivity.

3. The International Convention on Nuclear Safety

The apparent need to improve CANDU Large LOCA safety margins was raised in the Third Review Meeting of the International Convention on Nuclear Safety in Vienna in 2005. The known positive reactivity change following coolant voiding in CANDU reactors has been discussed at Convention review meetings and in other international forums for several years. Canada reaffirmed, at the 3rd review meeting, that NPPs in Canada meet all international safety requirements. The general perception that a positive void reactivity coefficient is a serious inherent weakness of any reactor design likely has contributed to the fact that the subject of CANDU Large LOCA safety margins has been raised during successive review meetings.

By the same token, an important inherent strength of the CANDU design, namely, its relatively long neutron lifetime, has not been sufficiently well understood by the international community. Because each reactor type has a combination of beneficial and detrimental characteristics, and because each design incorporates engineered design features to compensate for these limitations, it is important to review this particular area in a balanced and factual manner when attempting inter-comparison of the overall safety of different reactor types.

While Canada's statement that CANDU reactors already meet international design and safety standards has not been called into question explicitly by parties to the Convention, a question on the need to improve one of the safety requirements (Large LOCA margins) has been raised. Subsequent to the 3rd Review Meeting, Canada made a commitment in the follow-up anniversary report to "continue the program to improve Large LOCA safety margins" through two parallel approaches, viz., plant design changes and safety analysis tools/methodology improvements. The latter, in particular, includes development of best-estimate and risk-informed methodologies

consistent with the CNSC Executive's strategic direction towards a more risk-informed approach to resolving outstanding safety issues. Progress on this commitment was reported by Canada at the 4th Review Meeting in April, 2008. Discussion of the issue has been prominent in other international forums, such as the recent CANDU Owners Group TCM in Romania. [4].

Resolution of the Large LOCA margins issue principally relates to Article 6 (Existing Nuclear Installations) and Article 14 (Assessment and Verification of Safety) of the International Convention. Implicit in Article 6 of the Convention is the need to "upgrade" the safety of each existing plant when necessary in the context of the Convention. This sentence implies the need for comparison of a plant's level of safety against an agreed set of standards such as those developed by the IAEA. The IAEA documents are intended to be solid consensus standards based on common worldwide approaches.

This paper undertakes a simple analysis of only one aspect of this comparison – the fuel energy input during the first few seconds of those RIA transients unique to each reactor type. This first step is essential to consideration of safety margins, because to seriously consider safety margins one must first define what is meant by the term; that is, to answer the question "Margins to what limit?" Both probability and consequence of failure (i.e. both frequency of occurrence and the consequence of exceeding the limit) form part of this answer. Provided the particular reactor being considered exhibits safety performance similar to other reactors existing at the time the Convention entered into force, it is reasonable to conclude that no "upgrade" is then required within the context of the Convention.

Canada is aligning with international approaches [e.g. 5, 6] in these areas (Probabilistic Risk Assessment, Periodic Safety Review, and Risk-Informed Decision Making). With respect to Large LOCA issues, better refinement of the safety margins and more accurate value-impact assessments are expected as we align with the international approaches. Although improvements have been made, and although the overall risk remains small when all aspects of improved knowledge are considered, further work is in progress to examine potential improvements to Large LOCA safety margins through the parallel approaches of plant design change (specifically new fuel and safety system designs), and safety analysis/methodology development.

In the international context resolution of the issue of Large LOCA safety margins will rest on the fact that existing CANDU reactors are not only adequately safe when compared with international standards, but that all "reasonably practical improvements are made" to increase safety margins.

This paper addresses the first of these issues, and the companion paper in this session presents the current approach to the second issue.

4. Margins to Safety Limits

Both the frequency of occurrence of close approach to a specific defined limit and the consequence of exceeding that limit are important to a discussion of safety margins.

Knowing an approximate frequency of occurrence is important because of the working definition of safety as the inverse of risk. Risk is in turn defined according to the normal practice of insurance actuaries and nuclear safety specialists, as the product of frequency and consequence.

Consequence is easily defined as the result of exceeding a given safety limit. However, in any deterministic analysis the difficulty lies in finding ways in which the defined limit might be exceeded. In this analysis, the general approach is to examine all the known means through which the calculated consequence is controlled; that is, how is the parameter in question maintained below the limit? For example, the means may be via inherent reactor characteristics, by action of engineered systems, or by adequate depth of shutdown.

Then we find the most important "next failure" that involves postulated inaction of the controlling mechanism. Knowledge of the conditional probability of the "next failure" is, of course, essential to this process.

5. Case Study Framework

Given the limitations in the scope of work, our choice was to select published information from sources mainly associated with license applications of the various reactor types. It is realized that this choice introduces uncertainties in modeling such as the degree of conservatism forced on the analyst by regulatory rules; or more specifically, the differences in these rules between various jurisdictions. From previous experience it was decided that this uncertainty could be neglected because of the relatively uniform conservative assumptions required among the world regulatory agencies. Some specific exceptions are noted in the following descriptions.

Selection of specific cases began from the first postulate of some malfunction that could lead to a substantial positive reactivity insertion. A search of the literature revealed a limited number of well-documented cases. It was decided to choose cases describing these events in reactors that have already been constructed and licensed, or that are now in the late stages of preparation for construction.

The primary correlating parameter of the various RIA cases is fuel enthalpy. In both LWR and CANDU reactor designs, accidents that result in a rapid positive reactivity addition terminated by shutdown are characterized by an "integrated energy addition" to the fuel during the power transient. This power transient is typically no more than about 2 seconds in duration, and since fuel cooling is negligible during this time, the energy addition is well approximated by the time-integral of the fuel power transient.

Since the power decreases very rapidly after shutdown occurs, the total fuel energy (or enthalpy) reaches a maximum value within a few seconds. This result is expressed as a "peak radial average fuel enthalpy" as this is the value that has been shown to determine the degree of fuel damage in numerous RIA tests performed on LWR, VVER and CANDU-type fuels in various research reactors. For ease, the "peak radial average fuel enthalpy" will be referred to henceforth as "peak enthalpy".

5.1 Specific Comparison Cases

The reader is reminded that the following comparison has only a narrow and specific scope and that it makes no claim for or against the overall safety of any of these power plant designs. All of the postulated accident cases discussed in this Section incorporate engineered systems (shutdown, containment, and long-term heat removal) to render the plant safe. All of the plants discussed, and many other plants of the same type or class, have been judged to be adequately safe by regulatory authorities in a number of countries. Furthermore, extensive worldwide operating experience with the current generation of these plant designs has fully vindicated this regulatory judgment.

The selection of extreme cases presented tends to hide a very important fact. This fact is that the accidents described here are extremely unlikely, and the assumptions and methods leading to the behaviours described here are deliberately arranged so that the event consequences are maximized, or at least made more damaging than would be expected in the real world.

Short-term power histories for each of these cases are shown in the multi-part Figure below.

5.1.1 TMI-1 main steam line break (MSLB-FP)

The TMI MSLB event was chosen for comparison because the event begins with the PIE ‘rupture of a large coolant pipe’. The information for this case is taken from an OECD/NEA benchmark problem solved at a number of laboratories. [7] Flashing on the secondary side of the broken steam generator results in rapid cooling of the primary coolant, the rate and magnitude depending on assumed closure or non-closure of isolation valves.

There is a time delay of a few seconds before cold primary water enters the reactor, during which time reactor trip signals are issued. Shutdown rods begin to enter the core 7.5 seconds after the event, at which time the peak total reactivity is about +1 mk and peak power is about 1.25 times full power. Peak enthalpy does not change significantly; it remains at approximately 450 J/g. Shutdown rod insertion decreases the reactivity by about -40 mk at 10 seconds post-break.

Total positive reactivity added (from primary side cooling and fuel cooling) is about +15 mk at 10 seconds after the event, and about +40 mk after 50 seconds. Total reactivity rises slowly and returns to near zero approximately 50 seconds after the pipe break. The overall result is sensitive to reliable and timely control rod action. Reactor power would rise rapidly if rod insertion were appreciably delayed. Negative Doppler feedback would effectively limit the resulting power transient. Maintaining the reactor in a subcritical state during long term cool-down likely would require action of a secondary shutdown system.

5.1.2 ESBWR generator trip with failure of steam bypass (GTFSB-FP)

This event was chosen because the transient is very fast and because control response must be equally fast in order to prevent insertion of a large positive reactivity. An anticipated transient (generator trip) precedes the ESBWR PIE. The positive reactivity addition is caused by collapse

of steam bubbles resulting from the transient overpressure. Timing of the overpressure is determined by the travel time of the pressurization waves from the closing valve to the reactor core. Turbine stop valve closure is initiated at time zero by the generator trip signal, and is completed after 0.1 seconds.

The PIE begins with total failure of turbine bypass valves to operate in response to the generator trip signal. A reactor trip signal is initiated at 0.15 seconds and the rods begin to enter the reactor at 0.4 seconds. Peak reactor power of 2.5 times full power is reached at 0.8 seconds. Rods are fully inserted after 3 seconds, thus rendering the reactor safe (provided that long term fuel heat removal is available). Void collapse results in a reactivity increase of +5.53 mk during the first 0.6 seconds. Control response returns the total reactivity to about zero after 0.9 seconds. Reactor power rises very rapidly as the turbine stop valve closes, and then decreases. Doppler feedback reactivity is slightly positive beyond 5 seconds due to cooling of the fuel. Control response acts very rapidly to limit the peak total reactivity to 2.8 mk at 0.6 seconds, and continues to add negative reactivity until it reaches –166 mk after 3.5 seconds. Peak fuel enthalpy is 395 J/g. Positive reactivity (from void collapse) is about 37 mk at 8 seconds following the generator trip.

5.1.3 AP1000 cluster control assembly ejection, full power start of cycle (RCCA-FPBOC)

This event was analyzed by the designer. Results are published on the website of the US Nuclear Regulatory Commission [9]. As is usual in licensing analyses, a number of conservative assumptions are made to give assurance that an actual rod ejection event would be less severe than the one analyzed. The frequency of this PIE is judged to be extremely low.

Control assembly ejection is a very fast event. Peak total reactivity is approximately 3.5 mk at 0.14 seconds under full power beginning of cycle conditions (delayed neutron fraction 4.9 mk). The resulting power pulse is reversed by Doppler feedback and then shutdown rod insertion begins at 0.93 seconds. The hottest fuel experiences less than 10 percent melting. Peak fuel enthalpy at the hot spot is 758 Joules/g.

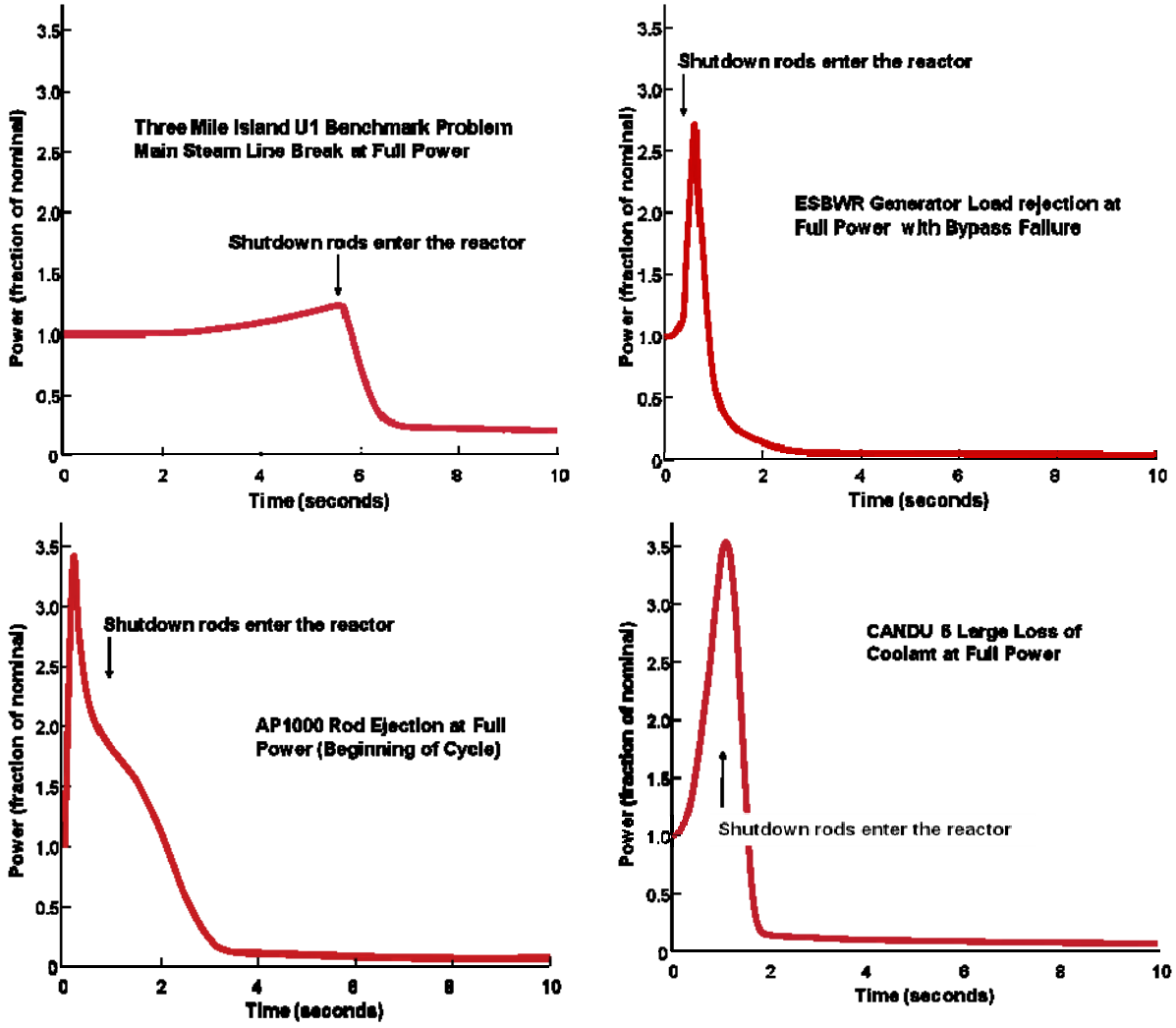
A second analysis was carried out for AP1000 at initial conditions typical of zero reactor power at the end of an operating cycle. The main difference in this case relative to the full power case is that the ejected rod has a larger positive reactivity, as calculated for the maximum allowed rod insertion at zero power level. The control rod positive reactivity in this case is considerably larger than the delayed neutron fraction. Of course, the fuel is cooler than it is at full power because the unit is at zero power in this case.

The case illustrates the effect of the short prompt neutron lifetime of the PWR, and the resulting mitigation of the power increase by the Doppler feedback. Reactor power rises extremely fast, through many decades in a small fraction of one second. Peak power of approximately 15 times full power is reached at 0.27 seconds. Shutdown rods begin to enter the reactor at 1.13 seconds. The peak total reactivity is estimated to be approximately equal to the delayed neutron fraction of 4.4 mk under these conditions. The peak fuel temperature is 1795 C at about 2.9 seconds. Peak fuel enthalpy at the end of the transient is 490 Joules/gram, below the expected fuel failure threshold.

5.1.4 CANDU 6 large loss of coolant (LLOCA-FP)

The CANDU Large LOCA case was chosen because the event begins with the PIE 'rupture of a large coolant pipe'. This particular case depicts the relative peak bundle power following a 100% break in a coolant pump suction pipe. At the same time analytical models of the transient thermal-hydraulics of the system are chosen to be conservative in the sense of producing the maximum calculated coolant voiding effects.

Within 2 seconds following a sudden break in a large primary circuit pipe, steam is produced in the reactor core and liquid coolant is ejected from both ends of the fuel channels. Trip signals (high neutron flux and high rate of change of the logarithm of the flux) are issued about 400 milliseconds following the event, and rods begin to enter the core at 0.9 seconds. Peak power of 3.5 times full power is reached at 1.16 seconds, after which either SDS1 or SDS2 decreases the



reactivity to -69 mk or more after 2 seconds. The peak total reactivity is +4.3 mk at 0.9 second (compared with the delayed neutron fraction of 5.2 mk) and the peak enthalpy is 638.5 J/g; Doppler feedback is small and negative. The total positive reactivity addition is about +15 mk at

10 seconds after the event. Final shutdown is reached at 2 seconds after the event, so that (with assistance from other engineered safety actions such as emergency fuel cooling) the reactor is rendered safe.

5.2 Hypothesized "Next Failure" Consequences

The experience from historical extreme events [10] indicates that improbable combinations are likely to have "fat tails"; that is, they show non-Gaussian probability distribution on the wings. Reactor accident analysis involves, by and large, examination of the consequences of such extreme events, without close examination of their associated probability.

The resilience of predicted limit-consequences of any accident sequence can be tested by postulating a series of "next failures" and estimating their consequences. This is sometimes referred to as testing "cliff-edge" effects in accident analysis. This method was applied by the AECB some years ago in the context of CANDU licensing proceedings.

Applying this idea to the cases selected here leads to the following observations.

Control rod ejection is an unlikely event in a properly maintained PWR. However, the severely degraded condition of the Davis-Besse vessel head brought the possibility of such an event into sharp focus and led to extensive inspection and correcting actions at several similar plants around the world. With reference to section 5.1.1, the most immediate "next failure" might involve the ejection of more than one rod cluster, leading to positive reactivity addition well in excess of the delayed neutron fraction.

Rod ejection from zero power shows similar behaviour to the full power case, except for its faster power rise and consequent possibility of fuel shattering.

Main steam line break in a PWR is well controlled, provided one assumes successful closing of isolation valves in the unbroken steam lines, so that the speed and magnitude of primary water cooling is limited. The "next failure" might involve the valves remaining open, or might arise from delay or failure of borated water injection within the next few seconds. Either of these events would result in a super-prompt-critical transient with substantial fuel temperature rise and negative Doppler feedback. Long term fuel cooldown as well as sustained high boron concentrated in the core water would be essential to render the reactor safe.

A major pipe break in CANDU6, assumed to occur instantaneously at time zero, is well controlled by either shutdown rods or by liquid poison injection into the moderator. The "next failure" may be complete failure of one shutdown system. In such an event, the independent second shutdown system would operate, leading to rapid shutdown. Long term cooling by ECCS water would render the reactor safe, especially because the light water emergency coolant acts effectively as yet another source of negative reactivity. Even in the event of complete failure of the ECCS, rejection of heat to the moderator water would prevent fuel melting. In CANDU 6, a steam line break would produce a negative reactivity transient. In fact, the resultant cooling of

primary water has a beneficial effect on safety in case of a large LOCA event, as it aids the injection of ECCS water.

Failure of steam bypass in the ESBWR is well controlled by shutdown rods, and essentially no fuel overheating occurs. In this case the "next failure" may be a delay in shutdown action, by 250 milliseconds or more. In such a case very rapid fuel heating would occur, with positive reactivity addition several times larger than the delayed neutron fraction at about 1 second. Negative Doppler reactivity would tend to reduce this reactivity addition, but fuel shattering and melting may occur. In any case, long term cooling would be essential to render the reactor safe.

In general, the consequences of "next failure" events in CANDU 6 are less than those in both the PWR and BWR.

6. Conclusions

All of the accidents here outlined involve rapid reactivity increases that might, if unchecked by engineered systems, lead to severe core damage in the long-term. Each of these reactivity increases is terminated one way or the other, and the reactor is rendered safe, by fast-acting shutdown mechanisms combined with engineered systems that provide long-term fuel cooling. The details of the event sequence, specific to each reactor type, is subject to further study as not all the information is available to the authors, particularly for plant designs other than CANDU with which the authors are familiar.

The next stage of comparison must involve the probability of occurrence of the event, as well as the conditional probability of occurrence of the "next event". This conditional probability depends on the reliability and speed of the shutdown mechanisms that accomplished the shutdown in the reference case. The final stage is to estimate the consequences of failure following the "next event". These consequences might range from safe, stable, shutdown conditions to more serious consequences such as fuel melting and release of large quantities of volatile fission products inside the containment. Under these very severe conditions the AP1000 incorporates an ex-vessel cooling system that converts the pressure vessel into a "crucible" that can stabilize and cool molten core debris in the bottom of the pressure vessel. This new design feature is conceptually similar to the severe accident cooling provided passively in CANDU reactors. In CANDU, the moderator water and the cool shield tank water surrounding the fuel channels also are fully capable of long-term (several days) stabilization of reactor core debris.

Transients submitted for licensing approval are unlikely to represent a true prediction of the event sequence being studied, because of the several "conservative" assumptions made in the models and constitutive equations. Modern analyses are trending toward more realistic models backed up with explicit provision for uncertainties. The authors of this paper expect that the calculated consequences of all RIA events in these plants will become less and less severe as these predictions become more accurate. Eventually, it is expected that CANDU reactors will be proven to be incapable of producing severe health consequences to surrounding communities.

7. References

[1] Ajit Muzumdar, Daniel Meneley, “Large LOCA Margins & Void Reactivity in CANDU Reactors”, Report COG-07-9012 (August 2007)

[2] “Safety of Nuclear Power Plants: Design”, International Atomic Energy Agency, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[3] “Convention on Nuclear Safety”, http://www.iaea.org/Publications/Documents/Conventions/nukesafety.html Vienna, 2008

[4] “ Technical Committee Meeting, Romania”, CANDU Owners Group, 2008 (private communication)

[5] “European Safety Practices on the Application of Leak Before Break (LBB) Concept”, The Nuclear Regulators’ Working Group Task Force on Leak Before Break, EUR 18549 EN, Final Report, (Jan 2000)

[6] “Risk-Informed Regulation of Nuclear Facilities: Overview of the Current Status”, IAEA-TECDOC-1436, February 2005.

[7] Pressurized Water Reactor Main Steamline Break (MSLB) Benchmark, NEA/NSC/DOC(2003)21, NEA Nuclear Science Committee (2003)

[8] ESBWR Design Control Document, Tier 2, Chapter 15, Safety Analysis, GE Nuclear Energy. 26A6642BP, Revision 2, (Oct 2006)

[9] “CONTROL ROD EJECTION”, AP1000 Design Control Document, Revision 15, Westinghouse Electric Company, 2005

[10] Nasim Taleb, “The Black Swan, The Impact of the Highly Improbable” Random House, 2007, ISBN 978-1-4000-6351-2