

Directorate of Power Reactor Regulation

April 7, 2008

E-DOCS #3232348 / 2.01
(26-1-8-1-8)

Mr. D. Patrick McNeil
Senior Vice President
New Generation Development
Ontario Power Generation
889 Brock Road
Pickering, Ontario
L1W 3J2

Dear Mr. McNeil:

Subject: CNSC Staff Review of Pickering NGS-B Integrated Safety Review – Safety Analysis Safety Factors Report

CNSC staff has completed the review of the Safety Analysis Safety Factors Reports [1], which addresses the three safety factors related to the safety analysis subject area, namely, Deterministic Safety Analysis, Probabilistic Safety Analysis and Hazard Analysis.

CNSC staff has focused the review of the above report towards the expected elements based upon the guidance provided in IAEA NS-G-2.10 [2], regulatory document RD-360 [3], and OPG's ISR Basis document [4].

CNSC staff have numerous comments, which are included in Attachment 1, with regards to:

- Completeness and Comprehensiveness of the Safety Report
- Fuel and Reactor Core Nuclear Design
- Shutdown System Effectiveness
- Reactor Regulating System
- Dose Acceptance Criteria/Dose Limits
- Initiating Events
- Containment Performance
- System Performance Issues
- Pickering B Risk Assessment
- Hazard Analysis
- Quality of the Safety Factor Report

Final conclusions on the adequacy of Safety Analysis will not be made until the Safety Factor report on the Actual Condition of SSCs is reviewed, and those results considered in the review of the Safety Analysis Safety Factor report.

CNSC staff does not recommend acceptance of the Safety Analysis Safety Factors report at this time.

CNSC staff will track our final comments, Attachment, in accordance with Reference 5. However, since three reports have been combined into one report the comments are numbered using the unique safety factor number of "5" only instead of "5, 6, and 7". We request that you send a response acknowledging your acceptance of these comments, using the assigned numbers, including acknowledgement that they will be incorporated in the final ISR Report, the Global Assessment and the Integrated Implementation Plan.

Yours truly,

T.E. Schaubel
Director
Pickering Regulatory Program Division

cc: A. Omar, D. Miller, Pickering Site Office

Attachment (1)

References:

1. Letter from D. Patrick McNeil to T. E. Schaubel, "Pickering NGS-B – Integrated Safety Review – Safety Analysis Safety Factors Report", June 29, 2007, E-Docs # 3063118.
2. International Atomic Energy Agency Safety Guide No. NS-G-2.10, "Periodic Safety Review of Nuclear Power Plants", Vienna, 2003.
3. Canadian Nuclear Safety Commission, "Life Extension of Nuclear Power Plants", Regulatory Document RD-360, February 2008.
4. Ontario Power Generation, "NGD Integrated Safety Reviews", N-PROC-LE-0001, July 2007.
5. Letter from T. E. Schaubel to D. Patrick McNeil, "Pickering NGS-B – Integrated Safety Review – Tracking of CNSC Comments from the review of ISR Safety Factor Review Reports", May 15, 2007, E-Docs # 3047770.

ATTACHMENT 1

Pickering NGS-B Integrated Safety Review – Safety Analysis

5.1 Summary

CNSC staff has reviewed the Ontario Power Generation (OPG) submission containing their Integrated Safety Review (ISR) Safety Factor Report on Safety Analysis [1].

CNSC staff has focused their review of the ISR Safety Factor Report on Safety Analysis [1] towards the expected elements based upon the guidance provided in IAEA NS-G-2.10 [2], regulatory document RD-360 [3], and OPG's ISR Basis document [4].

CNSC staff have comments with regards to:

- Completeness and Comprehensiveness of the Safety Report
- Fuel and Reactor Core Nuclear Design
- Shutdown System Effectiveness
- Reactor Regulating System
- Dose Acceptance Criteria/Dose Limits
- Initiating Events
- Containment Performance
- System Performance Issues
- Pickering B Risk Assessment
- Hazard Analysis
- Quality of the Safety Factor Report

CNSC staff conclude that:

- The safety analysis safety factor report is incomplete and requires further work. This should involve not only addressing the CNSC staff's findings adequately, but also involve additional safety analysis and, to the extent practicable, implement design and operations modifications to address all identified shortcomings.
- The information on fuel and reactor core nuclear design in Safety Analysis Report and supporting references is fragmented, incomplete, and the values of key basic nuclear parameters are based on obsolete information and neutronic methods and computer codes which are no longer supported by OPG.
- The impact of fuel and reactor core design parameters which are different from values at the time of original licensing on design control parameters for control and safety systems has not been discussed in reference 1.

-
- The existing outstanding safety issues related to effectiveness of shutdown systems have not been discussed in OPG assessment. Among the most significant outstanding issues are:
 - SDS1 reactivity depth;
 - Shutdown systems effectiveness for reactivity and power mismatch transients;
 - Shutdown systems effectiveness and large LOCA safety margins.

 - There has been no systematic analysis of the capability of the control system to cope with AOOs as required by modern standards.

 - We cannot confirm OPG conclusion that the deterministic analysis as it is documented in the current Safety Report is conformant to the modern codes and standards. This is because:
 - a significant part of the analyses in the Safety report was performed with computer codes which were not demonstrated to be applicable, e.g., validated, verified, subjected to quality control or properly documented;
 - some analyses, performed at the time of original licensing do not consider effects of design modifications, plant aging or changes in operating limits and conditions;
 - some of the initiating events, which should be considered according to the modern requirements, have not been analyzed. This includes whole categories of events such as beyond design basis accidents, as well as accidents initiated by human errors, and external and internal common cause events;
 - for several events in the current Safety Report it was not possible to demonstrate compliance with radiation dose limits in modern standards;
 - application in safety analysis of the single failure criterion is not rigorous and is not in conformance to the modern requirements;
 - OPG's assessment of deterministic safety analysis area is incomplete and lacks adequate depth. The deterministic safety analysis for Pickering B refurbishment needs to be carried out anew using the modern day knowledge, actual description of Pickering B fuel and reactor core nuclear design, feedback from operating experience, state of the art models and computer codes, generally accepted standards and best practices. This can be done as part of RD-310 implementation.

 - The safety factor report [1] fails to identify the need to assess containment performance for severe accidents and to consider design changes to manage severe accidents.

 - S-294 standard requires that a facility specific PSA includes internal and external events. Although this is a preferred approach for all events, the standard allows using alternative analysis with agreement of persons authorized by the Commission. PBRA considers currently only internal events. OPG claims that all other events have been addressed by alternative analysis. However, a comprehensive assessment identifying all potential initiating events, both internal and external on power and in shutdown state, applicable to the plant and mapping

these against available analysis to demonstrate a complete coverage has not been provided. Furthermore, OPG needs to seek CNSC's acceptance of the methodologies used for analyses not included in PBRA in the context of their contribution to the overall plant risk; however, OPG has not yet submitted the methodologies for CNSC acceptance. Therefore, we cannot confirm that the Pickering B safety analysis package meets S-294 requirements. Furthermore, since analyses of all initiating events, even those assessed with alternative methodologies, shall be subjected to S-294 requirements, these analyses shall represent the plant as build and as operated and be updated every three years or sooner. Apparently, this has not been done for the alternative analyses. These issues shall be identified as discrepancies

- Several discrepancies have been noted with regards to hazard analysis. In particular, issues regarding Fire Hazard Assessment (FHA) and the resulting Fire Safe Shutdown Analysis (FSSA), seismic qualification and its accompanying safety assessment, pipe rupture and flooding.
- Many reviews performed in this report are correct and identify existing issues as discrepancies for further resolution during the definition of refurbishment scope. However, CNSC staff disagree with a number of dispositions of direct compliances and acceptable deviations in which OPG states their position without substantiation, or make conclusions without confirmation.

5.2 Assessment Results

CNSC staff have comments with respect to:

- Completeness and Comprehensiveness of the Safety Report
- Fuel and Reactor Core Nuclear Design
- Shutdown System Effectiveness
- Reactor Regulating System
- Dose Acceptance Criteria/Dose Limits
- Initiating Events
- Containment Performance
- System Performance Issues
- Pickering B Risk Assessment
- Hazard Analysis
- Quality of the Safety Factor Report

In addition, comments on categorization of findings are provided throughout this report.

5.2.1 *Completeness and Comprehensiveness of the Safety Report*

Based on the review and past CNSC staff experience, many analyses supporting safety case of the plant and establishing requirements for Pickering B safety systems are

documented in reports not included in Safety Analyses. For instance, a number of design basis initiating events are assessed separately from the Safety Report. Safety Analysis conclusions rely also on other reports which may be difficult to obtain and, thus, trace fully the conclusions. There is no comprehensive reference document including all information on the plant safety assessment. It is very difficult to trace all of such reports if they are not referenced in one single place. In fact, the situation of having multiple different assessments not included in the Safety Report but documenting essential safety features of the plant creates significant difficulties in the regulatory oversight and in the maintaining the safe operation of the plant by the licensee. The full picture of the plant safety case is not transparent. As a result, OPG staff may not be aware of some of the important safety features in the day-to-day operation and CNSC staff may have difficulties in assessing plant safety without a comprehensive well traceable set of documents making the licensing basis. This issue is a **Discrepancy** and OPG is requested to compile a comprehensive set of documents, eventually a fully revised Safety Analysis report, addressing the Pickering B safety basis.

Specific examples include:

- Under qualification of safety analysis codes used in the Safety Report, it is stated, “Many legacy codes have not undergone complete verification and validation and these may need to be used to support safety assessments for life extension. Resolution of this issue may require gap assessments to be done to show that analysis results remain conservative. This issue is also identified as Acceptable Deviation against requirements from NS-R-1 (Clause 5.7).”
- It is stated in Reference 1, “The establishment and implementation of the Safe Operating Envelope (Operational Safety Requirements and Instrument Uncertainty Calculations) at Pickering B is considered to be a relative specific strength area for Pickering B. The rigorous process of developing the SOE resulted in the identification and reconciliation of many issues (gaps) in the safety analysis area. Recognizing that there are still some gaps relating to the program implementation, continued assessment of this program is key component in terms of ensuring full compliance with the Safety Analysis Safety Factor.”

It is difficult for the CNSC staff to accept this because their configuration management program is not complete, see action item AI-030502, and there appears to be no intent to update any safety analyses to ensure consistency between the safety analysis and the actual plant condition. The results of updated safety analysis should be transferred consistently to all relevant documents such as the OSRs, Operating Manuals, Maintenance and Surveillance Programs. All of the inter-related documents should be shown to be current and consistent. Compliance should be demonstrated. The consistency with the SAR of information at low-tier documents such as the OSRs, Operating Manuals, Maintenance and Surveillance Programs should be audited.

- Many of the OPG hazard assessments, such as for pipe rupture, seismic, turbine missiles, aircraft crash rely on “stand-alone analyses” performed in the late 1970’s

or early 1980's. OPG has not assessed that these stand-alone assessments remain valid according to current plant design, configuration or condition, or that they are valid for extended operating life, and current safety standards and operating experience. We consider these to be **Discrepancies** which recur in many areas throughout the report.

- Page 37, NS-G-1.2 Clause 4.45 (under NSR- 1 Clause I.7 in (Appendix D, Section D.2.1.1). OPG identifies that the common mode events such as fire, explosion, turbine missile impact and floods of internal origin are not included in the list of PIEs within the managed safety analysis program. Stand-alone assessments were completed for some of these events such as reactor building flooding (30-SDM-6), turbine missiles (REP-NA44-41000-8) and fire (NK30-REP-71400-00001). The stand-alone assessments are predominantly static documents that have not necessarily remained current with the plant design. OPG has classified this as a discrepancy. CNSC staff agrees this is a discrepancy, however we consider:
 - OPG should identify which specific common mode events are not included in the list of PIEs within the managed safety analysis program.
 - OPG should identify which specific common mode events are covered by “stand-alone assessments” and identify these assessments. OPG should review these and identify which of these are no longer valid or current.
 - OPG should revise the analysis for all operating modes, not just full power.
- Page 37, NS-G-1.2 Annex A-3. OPG identifies that some of the assessments that demonstrate that structures, system or components perform the listed safety functions are outside of the safety analysis. OPG claim, historically, some assessments were done outside of the Safety Report, but whenever these reports were submitted to the regulator they became part of the licensing basis. Based on this, OPG has classified this as an acceptable deviation.

CNSC does not concur with the classification as an acceptable deviation. OPG has stated that these stand-alone assessments are predominantly static documents that have not necessarily remained current with the plant design. OPG has not assessed that these stand-alone assessments remain valid according to current plant design, configuration or condition, or that they are valid for extended operating life, and current safety standards and operating experience. Therefore we consider this issue should be a **Discrepancy**.

- IAEA NS-R-1 Clause 3.10, p. 136: OPG states that they are in direct compliance with this clause yet CNSC staff evaluations have indicated that many stand-alone Safety Analysis reports do not reflect the current plant configuration. OPG's Plant Design Safety Factor Report [5] also acknowledges that design documentation does not reflect the current plant configuration. This issue clearly is a **Discrepancy**.
- IAEA NS-R-1 Clauses 5.7, 5.20, 5.71, A.3, p. 143, p. 147, p. 157-159, p. 172-173: OPG has indicated that they are in direct compliance or consider the issue to be an

acceptable deviation with all clauses, but OPG needs to compile all stand-alone documents (SDMs, D&D Reports) into an updated Safety Report.

- Human errors and common cause events as initiating events leading to accidents should be considered in the analysis according to NS-R-1 and NS-G-1.2. This is identified as “acceptable deviation” in OPG review since the Pickering B safety analysis does not include these kinds of events. In CNSC staff view, such events should be considered explicitly.

The scope of safety analysis expected as part of an ISR is broader than that performed as part of the “Safety Report Update Process”. The intent of ISR is to bring a plant built to old standards to a modern plant meeting modern standards to the extent practicable since the refurbished plant is intended to operate additional 30 years. For this reason, all additional events that were not covered in existing analyses, events that were analyzed previously using outdated models, GAIs and issues in the Reference Analysis Plan should be assessed or analyzed to determine if actual design improvements need be made.

For instance, it is expected that there will be:

- A review of gaps in trip coverage;
- A review for inconsistencies in analyses;
- A systematic re-assessment of initiating events;
- For each event to be included in the SR, a review of analysis assumptions;
- For each event analyzed, an assessment of how as-built plant conditions and present operational practices affect the safety cases; and
- Identification of design changes to make as part of life extension.

In summary, Pickering NGS B should submit a new safety analysis report to support the operating licence that demonstrates the adequacy of the design expected of a new NPP. Such safety report will confirm validity of the existing safety analysis taking into account actual plant design, actual condition of SSCs and their predicted end state, current methods, and current safety standards and knowledge. This may be done as part of RD-310 implementation.

5.2.2 Fuel and Reactor Core Nuclear Design

Notable omissions in the OPG assessment are the lack of an updated documented description of fuel limits and reactor core nuclear design. The information on fuel and reactor core nuclear design in the current Safety Analysis Report is outdated and based on neutronic methods and computer codes which are no longer supported by the original designer and OPG. The lack of full and accurate documented description of fuel and reactor core nuclear design is a significant safety issue in itself and indicative of a non-conformance with modern standards.

The fuel limits are essential in setting the success criteria for the control and shutdown systems. The absence of qualified fuel limits introduces significant uncertainty in the assessment of effectiveness of control and shutdown systems which is mainly based on

safety analyses. The need for solid experimental data, in particular in qualification of fuel, was highlighted in the OPG assessment, by the statement made on page 101, regarding availability of post-dryout heat transfer data for the 28-element bundle, for example. The experiments, on-going at the time of preparation of reference 1, produced unexpected results, having substantial impact on the safety case for Pickering units (refer to Section 5.2.11 for additional comments regarding these experiments and conformance with G-144).

The information on fuel and reactor core nuclear design in the current Safety Analysis Report and other supporting documents, such as the Reactor Physics Design Manual, is outdated and based on neutronic methods and computer codes which are no longer supported by the original designer and operators. The values of key parameters of a CANDU natural uranium reactor core nuclear design are presented in Table 1, as inferred from information scattered in various recent licensing submission. The specific information, for Pickering B reactors, based on the as built reactor core, fuel, primary heat transport system, permitted operating conditions, verified and qualified, should have been updated, and documented by the designer and operator and discussed in the OPG assessment [1].

Table 1: Currently Expected Best Estimate Values as Compared with Original Estimate Values for an Equilibrium CANDU Core

Parameter	Range of original estimates (neutronic design original methods and computer codes)	Range of current estimates (neutronic design current methods and computer codes (new Industry Standard Toolset reactor physics codes))
Full core void reactivity (mk)	9-11	14-18
Delayed neutron fraction (mk)	5.7-5.9	5.1-5.3
Neutron lifetime (ms)	0.9	0.77-0.8
Fuel temperature reactivity effect	Slightly negative	Slightly positive
Power coefficient of reactivity	\`zero	Slightly positive

The new estimates of basic core neutronic design raise the need to re-assess the consequences of an extended range of design basis accidents that could be aggravated by increased magnitude of positive coolant void reactivity and less favorable values of the other key neutronic parameters.

The limits and acceptability ranges for the nuclear parameters of the reactor core nuclear design cannot be retrieved from the available design documentation. Therefore, it is unclear if new predictions, based on more accurate tools, are within original design basis and adequacy of design of control and shutdown systems confirmed.

Larger prediction of void reactivity along with significantly different values for the other key neutronic parameters of the reactor core nuclear design show a higher than anticipated sensitivity to PIEs. It also shows a higher than anticipated reliance on shutdown function. This raises the need to reassess the engineering margins build into the design of the safety function.

The impact of the larger prediction of void reactivity on shutdown system effectiveness for AOOs and DBAs, and for large LOCA in particular are further discussed in Section 5.2.3 on Shutdown System Effectiveness. The impact of the larger prediction on the reactor regulating system is discussed further in Section 5.2.4.

It is expected that OPG will carry out a condition assessment and reconstitution of the reactor core nuclear design. Further information on information to provide regarding reactor core nuclear design is provided in Appendix 1.

5.2.2.1 Coverage over the Extended Operating Life

The core geometry changes in time due primarily to irradiation induced distortions. These include pressure tube diametric creep, channel sag and channel elongation. The effect of core geometry changes has not explicitly been covered in the current safety analysis. The following briefly discuss the potential impact on reactor core nuclear design and effectiveness of shutdown systems only.

Core geometry changes affect the performance and effectiveness of the Neutron Overpower Protection (NOP) system, which prevents the overpowering of individual channels, and control and shutdown systems.

Pressure tube diametric creep also results in the fuel bundle sitting at the bottom of an enlarged pressure tube, which results in a series of changes in physics and thermal hydraulics characteristics, including an increase in coolant void reactivity, azimuthally asymmetric element power distribution, coolant volume, sub-channel flow pattern, flow by-pass, critical heat flux and critical channel power.

Channel sag leads to lattice irregularities, which is equivalent to variations in lattice pitch. The spacing from a channel to its neighbors deviates from the original lattice pitch by the difference in the relative sag. Channel sag increases the distance that the shutoff rods have to travel to achieve an effective reactivity bite. This may lead to degraded shutdown system reactivity drop performance. Furthermore, channel sag leads to changes in the position of the in-core devices and detectors relative to the channels, which may have an effect on the flux shape and detector readings.

Channel elongation extends the free end of the pressure tube, and could lead to the bundles being shifted out of core towards one end. Differences in channel elongation and latch displacement could lead to uneven power distributions (axial flux tilts) which may impact the effectiveness of NOP system.

The ageing effects on the lattice structure should be accounted for in the models used in design, safety analysis and fuel management whether by explicit modeling or adequate uncertainty allowances to ensure adequate safety margins are maintained.

Regulatory documents R8, R9 and R-10 require that shutdown systems are effective assuming their minimum allowable performance. The minimum allowable performance should cover for the potential degradation due to irradiation-induced core geometry distortions.

Standard CAN/CSA-N286.7-99, "Quality Assurance of Analytical, Scientific and Design Computer Programs for Nuclear Power Plants," and CNSC Regulatory Guide G-149, "Computer Programs Used in Design and Safety Analyses of Nuclear Power Plants and Research Reactors", require that models and computers codes be validated for all modelled phenomena and applications. The lack of modelling and its effect (or lack thereof) has to be justified, or the uncertainties introduced are to be included in the assessment of the simulation results.

Current design and safety analyses have not, in general, included the effects of the irradiation-induced lattice-geometry distortions. While some significant effects, such as the increase in positive void reactivity, have been addressed in safety analysis of most limiting design-basis events, such as large break LOCA events, most of effects related to lattice-geometry distortions were judged to be of negligible magnitude and not included in the modeling or covered by explicit allowances.

The lack of experimental data and capability of the current design and safety analysis computer codes to model the geometry-distortion-induced effects make the justification of dismissing these effects difficult to support when adequacy of safety level over the full operating lifetime is to be assessed.

5.2.3 Shutdown System Effectiveness

The broader issue is the shutdown systems design capability of meeting the objective of its design safety function to:

- prevent unacceptable reactivity transients;
- shut down the reactor as necessary to prevent AOOs from leading to DBAs;
- shut down the reactor to mitigate the consequences of DBAs.

Additional background information on regulatory requirements and expectations regarding shutdown system effectiveness is provided in Appendix 2.

5.2.3.1 SDS1 Reactivity Depth

SDS1 reactivity depth has been an outstanding issue for all CANDU reactors. Specifically, the reactivity depth of SDS1 is not sufficient to maintain the reactor shutdown indefinitely for certain design basis events, such as single channel events leading to in-core LOCA. Acceptability for these events is justified by crediting operator action. The following

CNSC (AECB) documents address SDS1 reactivity depth:

- AECB-BMD 77-147 “Depth of SDS1 - A History”
- AECB-BMD 78-119 “Depth of SDS1 - Requirements of the Event of a Pressure Tube Rupture”
- AECB-BMD 78-119A (Appendix) “History of Licensing Actions Related to SDS1 Depth (Subsequent to BMD 77-147)”
- AECB-BMD 79-15 “Shutdown Depth for Darlington NGS”

The following recommendations for future plants have been made in AECB-BMD 79-15 “Shutdown Depth for Darlington NGS”:

- augmentation of SDS-1 depth to ~100 mk, or
- provide a shutdown margin >30 mk

The SDS1 reactivity depth is a design issue for which, based on guidelines in RD-360 related to assessment against modern standards, there is non-conformance with:

-
- Requirements in regulatory documents R-10 and R-8
 - Safety Criterion (100 mk SDS1 reactivity worth or at least -30 mk subcriticality) set in AECB-BMD 79-15

CNSC staff note that there are design solutions, including for existing reactors. CNSC staff also note that improvements to SDS1 by increasing the number of rods using the adjusters has been implemented before in Pickering A reactors. Reduction of number of adjusters from 21 to 16 (which makes available locations for additional SORs) has been implemented in Darlington reactors since mid '90. Therefore there is operating experience relevant for a core with reduced number of adjusters).

It is expected that OPG would have carried out feasibility studies for addressing this non-conformance by design safety improvements.

It is also expected that the supporting safety case will cover known issues related to epistemic uncertainties and assumptions, such as:

- number of damaged guide tubes (TUBRUPT validation, recent experimental results related to fuel-moderator interaction);
- failure of neighbor fuel channels (impact of existing issues and aging); and
- poison dilution.

5.2.3.2 Shutdown Systems Effectiveness for AOOs and DBAs

The potential demand on the shutdown function is high, mainly due to the following features of the nuclear design:

- no self-limiting capability, due to positive reactivity coefficients;
- the reactor regulating system is capable of mitigating most, but not all AOOs; and
- shutdown action demanded for a large spectrum of AOOs and design-basis events, due to high sensitivity to PIEs

Supporting analyses for a significant number of events have not been revised for a long time. In particular, in-core LOCA events, control failure initiated events, loss of reactivity events, and loss of flow events, should be revised to reflect the current knowledge related to nuclear design and analysis tools, and current requirements.

The overall methodology employed in current Pickering B safety analyses of many of the above mentioned events is implicitly conservative, but it is also too simplistic:

- The simulation model of reactor core behaviour is highly stylized: it is not adequate to demonstrate adequacy of reactor design due to spatial spectral and associated resonance absorption effects, reactivity spatial effects, flux spatial distortions effects which need to be modeled explicitly;
- There is no systematic effort to either determine or account for various modeling approximations. Some events are analyzed using a point kinetics model; however,

the uncertainty related to predictions by point kinetics model is unknown, for example;

- There is no systematic treatment of uncertainty in prediction of key modeling parameters and relevant sensitivity and uncertainties studies. The margins build into design to cover simulation uncertainties are unknown;
- Calculations in general are design-centre while certain operating parameters are set at extreme values with the implicit assumption that the resulting conservatism will adequately cover various effects which are ignored. With a mix of assumptions of differing conservatism, the overall degree of conservatism in the analysis is not known. and true margins to the acceptance criteria are not evident; the adequacy of safety margins is based to a large extent on reasoning;
- Models and computer codes are not in general adequately validated for the range of conditions before, during and at the end of the simulated event. Therefore the uncertainties associated with the code predictions are largely unknown;
- Certain very stylized models and assumptions do not allow identification of limits and conditions to define a safe operating envelope that can be complied with in operation;
- The simulations do not always cover all permissible operating conditions that may challenge the safety function. Low power operation and GSS are few examples.

5.2.3.3 Impact of a Larger Predicted Coolant Void Reactivity on Shutdown System Effectiveness for AOOs and DBAs

The recent findings related to magnitude of coolant void reactivity (CVR) and the other key parameters of reactor core nuclear design further emphasize the need for a comprehensive revisit of the safety case supporting the shutdown systems effectiveness for AOOs and DBAs. In general, the positive coolant void reactivity feedback characteristic can play a role in any coolant voiding situations while the reactor is maintained in the critical state. The significance of the role played by the positive CVR feedback depends on the magnitude and duration of coolant voiding in the particular situation or scenario.

Under normal operating conditions, the large positive CVR characteristic results in greater challenges to the reactivity regulating and control systems to monitor, detect and control the minor reactivity excursions that may arise as part of normal operations so as to maintain the reactor power and the flux shape in the core within specified ranges. At the same time, the large positive CVR characteristic also leads to greater challenges to the reactivity regulating and control systems to differentiate between minor reactivity perturbations that are part of normal operations from the more significant reactivity excursions that are associated with certain AOO, and to respond in a timely and effective manner to prevent unacceptable reactivity transients invoking mitigation action by the shutdown systems.

Under upset or accident conditions, the positive CVR feedback characteristic can play a more significant role in the safety performance because the magnitude and duration of the coolant voiding transients can be much larger than those encountered under normal operating conditions.

In those situations or scenarios in which effective shutdown of the reactor is assumed following a potential initiating event (PIE), the roles played by the positive CVR feedback characteristic in a particular scenario depend on whether the coolant voiding results from an increase in fuel heat generation (*e.g.*, LORC events), coolant flashing as a result of system depressurization (*e.g.*, LLOCA events), or a degradation in core heat removal (*e.g.*, LOF events):

- In coolant voiding scenarios involving an increase in heat generation, the impact of the positive CVR feedback is enhanced to some extent by the slightly positive reactivity feedback due to fuel heatup, pending the core burnup distribution (distribution of fuel isotopic number densities) at the time of the event.
- In coolant voiding scenarios involving degradation in core cooling and/or system depressurization, the impact of the positive CVR feedback is immediate and again its contribution to transient progression may be enhanced to some extent by the slightly positive reactivity feedback due to fuel heatup, pending the core burnup distribution (distribution of fuel isotopic number densities) at the time of the event.
- The LOF scenario illustrates an increased vulnerability of the design to accident scenarios which result in localized core voiding. The large positive CVR feedback characteristic together with the inherent delay in the detection of localized upset or accident conditions present an increased challenge to the safety systems to meeting the acceptance criteria.
- The large positive CVR feedback characteristic results in a tighter coupling between the different analysis disciplines and increases the complexity of the analysis methodology. The uncertainty in results of complex 3-D neutronic-thermal hydraulic coupled simulations is currently unknown due to lack of integral effect tests.
- There are a number of residual and emerging safety issues concerning the safety case in various AOO and DBA scenarios which result in coolant voiding.
- An ongoing safety concern is the robustness of the safety analysis results to various discovery or emerging issues. This problem is most severe in those accident scenarios, *e.g.*, LLOCA and single pump trip event, where the safety margins are already small.

The “closeness” of the coolant condition in the outlet header to saturation is a mitigating consideration. Pickering reactors are designed to operate with subcooled outlet headers. In general, the greater the subcooling, the greater would be the margin before the positive

CVR characteristic comes into play. This consideration, expected to be relevant under normal operating conditions, as well as upset or accident conditions, should be further justified.

Another issue which enhances the complexity of assessment of shutdown systems effectiveness is related to the adequacy of modelling of fuel bundle behaviour under high temperature conditions and, especially under large break LOCA conditions. Currently, the bundle is assumed to preserve its original geometry throughout the transient. The industry continues to apply the prevention of sheath melting as an acceptance criterion for demonstration of the bundle coolable geometry. The safety analysis of LBLOCA shows that fuel experience temperature transients in the range for which no CANDU-prototypical experimental corroboration exists. The modelling of fuel bundle behaviour in the high fuel temperature range is lacking adequate validation and the credibility of code predictions under such conditions is low.

In certain high temperature accidents fuel coolability cannot be assured even upon initiation of the ECCS due to the fuel geometry changes and changes in material properties.

In all accidents with reactivity excursions, additional energy is deposited in fuel during a relatively short power pulse. In the limiting reactivity transients considered in design, the peak element power may reach 6-12 times the full nominal element power. Duration of the power pulse is in the order of approximately 2 s long and must be terminated by shutdown systems because the positive coolant density reactivity feedback would only exacerbate the power transient.

At a certain level of energy deposition fuel cladding would fail; at higher levels of energy deposition, both fuel matrix and cladding can be fragmented. As the fuel burn-up increases, such failures can occur at lower levels of the deposited energy. While CANDU fuel has lower burn-up, there are features which can potentially make CANDU fuel more susceptible to failures in reactivity transients, namely the thinner sheath, absence of the pellet to sheath gap, absence of the gas plenum in fuel elements. There currently are not enough data to understand the influence of these parameters on CANDU fuel behaviour in power pulses.

To sum up, in power pulse transients CANDU fuel can experience failures due to mechanisms which are not fully understood, due to lack of relevant experimental data.

The above issues are expected to be accounted for in the setting of safety criteria for effectiveness of shutdown systems.

5.2.3.4 Shutdown Systems Effectiveness – Large LOCA Margins

The LLOCA scenario represents a particularly challenging accident scenario since a single failure can result in the simultaneous occurrence of severe degraded core cooling and severe positive reactivity insertion from the coolant voiding behaviour following the large break. The initial phase of a LOCA for the currently operating CANDU reactors is

characterized by predictions of a significant power pulse. This leads to additional energy deposition in the fuel which enhances the fuel overheating due to degraded cooling conditions. The positive reactivity transient enhances the mismatch between power generated in the fuel and heat removed from the core and could lead to severe core damage and early challenge of containment integrity if not arrested in time.

The shutdown systems effectiveness to mitigate a LOCA event must be demonstrated, in accordance with an acceptable evaluation model, for a number of postulated breaks of different sizes, locations, and other properties, sufficient to provide assurance that the most severe credible consequences have been identified and are acceptable. Acceptable consequences means that the dose limit would be satisfied assuming no failure of the other special safety mitigation systems (ECCS and containment).

The consequences for a LOCA design basis transient have been calculated with more or less detailed simulation models using safety criteria and safety analysis computer models which were allowed to be as realistic as the database and experimental information base would allow.

Over time, a number of discovery issues, including unanticipated phenomena and design under predictions of certain nuclear design key parameters, such as void reactivity effect, have led to erosion of safety margins. The safety margins in the current safety case are reduced from the original safety case, due to higher predictions of energy deposition in the fuel during the power pulse and the design basis envelope has shrunk, due to more restrictive limits imposed on operating conditions and shutdown systems performance imposed to compensate for impact of discovery issues.

Following the 2001 reactor physics code replacement finding, all CANDU stations were required to demonstrate that the conclusions of the safety analysis remain valid. In other words, all stations were required to confirm adequacy of the implemented compensatory measures, i.e., to show that the conclusions of the analyses, reported in the safety reports, still conform to licensing basis.

Pickering B was the last station for which a detailed LBLOCA analysis with the new suite of codes has been performed. The priority of the re-analysis was low because of the large margins predicted in the earlier analysis.

However, the new analysis has resulted in prediction of consequences which are substantially worse than reported previously. For comparison, preliminary results (April 2005, reported in S-99 report P-2005--06880WER), current licensing case (submitted in 2000) and Pickering A LBLOCA results are given in Table 2.

Changes in the analysis assumptions, compared to 2000 Pickering B LBLOCA analysis, which may have a large impact on the results are as follows:

1. Use of the current IST code suite – notably, the change from SMOKIN to WIMS – this would lead to more severe predicted consequences with other conditions unchanged.

2. 200 ms faster SOR gates (this is the only compensatory action taken at Pickering B in 2001) – this would lead to less severe consequences.
3. Higher average core burnup.
4. Different time constants for the SDS1 HLR trip – for 100% RIH break the HLR trip comes in at 0.495 s (earlier at 0.446 s) – about 50 ms later.

An issue concerning the representation of HLR trip time constants/delay for Pickering B in LBLOCA analysis was raised since 1996. There is an on-going OPG project to better measure and represent various time components of SDS trip chain.

Table 2: Pickering A and B Major LBLOCA Analysis Parameters (new Pickering B results as per in S-99 report P-2005--06880WER)

	PB 100% RIH, 2000	PB 100% RIH, 2005	PA 100% RIH	PB 40% RIH, 2000	PB 45% RIH, 2005	PA 40% RIH
Bundle enthalpy, kJ/kg	663	843 (+27%)	562	600	752 (+25%)	543
Bulk Neutronic power	3.847	5.94 (+54%)		3.198	4.87 (+52%)	2.24
Net reactivity, mk	4.233	4.68		4.095	4.87	3.21
Centerline temp, C		2406	2138			
Sheath temp, C					1446	1468
HLR trip	0.446	0.495		0.597	0.592	

The new verified results reported in S-99 follow-up report P-2005-06880AR1 are given in Table 3.

Table 3: New Pickering B Verified Results per S-99 Follow-up Report P-2005-06880AR1

	PB 100% RIH, 2000	PB 100% RIH, 2005
Bundle enthalpy, kJ/kg	663	722 (+8.9%)
Bulk Neutronic power	3.847	5.77 (+49.9%)
Net reactivity, mk	4.233	4.62
Hot Channel Energy (MJ)	48.2	62.5 (+29.7%)
Bulk Integral (Full Power Seconds)	5.29	6.65 (+25.7%)
HLR trip	0.446	0.476

Although the verified 5-second physics results remained higher than presented in 2000 licensing analysis and results at Pickering A, OPG concluded that the impact is considered to be acceptable and safe operation limits of Pickering B units continues to be supported under existing licensing basis. The final results related to peak fuel centerline and sheath temperature have yet to be available, but OPG staff does not expect them to be significantly different from the preliminary results since April 2005 (see Table 5). The Pickering B LOE analysis is now planned to be completed and submitted with a BEAU analysis in early 2008, according to S-99 follow-up report P-2005-06880AR1.

CNSC staff opinion the new analysis indicates a significant change in the licensing case results and large reduction of the previously reported safety margins, as well as when compared with Pickering A licensing results. The reported results represent a significant increase in the consequences (50% increase in the predicted bulk neutronic power). Moreover, they potentially invalidate large parts of the licensing analysis documented in the Safety Report, in particular, the moderator subcooling calculations, containment analysis and assessment of radioactive releases and population doses.

In addition, The ECC effectiveness criteria given on page 162 of [1] (prevention of fuel melting, prevention of sheath melting) are not acceptable to CNSC.

CNSC staff remain concerned with the trend in erosion of safety margins, given the several generic issues, and expect that OPG will address the identified outstanding issues, and, in particular, will develop and implement engineered solutions to re-establish robust safety margins.

5.2.4 Reactor Regulating System

The OPG submission does not include a discussion of the capability of the control system to cope with AOOs, as required by modern standards. Item (3) of clause 4.1 in IAEA NS-R-1, relates to the second level of defence in depth: control of transients using inherent and engineered safety features. Since this level of defence in depth has not received detailed scrutiny under the Canadian regulatory regime, a discussion of this aspect should provide more supporting details. The discussion should:

- Acknowledge the positive power coefficient and, especially, positive void reactivity feedback which is a significant shortcoming in terms of inherent safety features;
- Provide supporting reliability information; operating experience has revealed an increase in number of RRS related events which is indicative of less than expected reliability of the system as well as higher than expected frequency of precursors and serious process failure events. Many were caused by equipment related issues, the dominant equipment related causes being equipment performance, and design configuration and analysis;
- Provide supporting details for the frequency of serious process failures.

Accepted current practice in Canada is that the control system, the Reactor Regulating system, is not designed to cover all AOOs. For the remainder of the AOOs, protection is provided by the two shutdown systems. The speed and depth of shutdown systems are greater than that of either the setback or stepback, so protection is provided. This type of protection arrangement is generic to all CANDU reactors.

Assessment against modern standards, including IAEA NS-R-1, indicates that this type of protection may be weak in that the second defence-in-depth line has limited capability in prevention of anticipated reactivity transients to escalate to unacceptable reactivity transients requiring quick mitigation action by the shutdown systems.

CNSC staff expect that OPG will carry out a comprehensive study of RRS design to adequately evaluate the actual level of safety of Pickering B design. The scope of the study should cover, among others, the following issues:

- Design basis and implementation of fail safe concept
- Design configuration, design specification and analysis
- Reliability analysis, ranking of key components
- Operating practices, experience and results of system health monitoring programs
- Current status of all components, including computers
- Probability of loss of regulation events based on actual design, condition of components, and operating experience
- Identification of the AOOs for which the control system has been designed to be effective (the design set of events)
- Justification for the AOOs not covered by the reactor control system (these cases should be taken into account in estimates of frequency for shutdown demand and assessment of the design reliability requirements for shutdown systems)
- Confirmatory deterministic analyses for all AOOs identified in the design set of events, including control requirements analyses (including setback and stepback analyses) and core stability analysis.

The following guidelines in the industry standard CSA/CAN3-N290.4-M82, "Requirement for the Reactor Regulating Systems of CANDU Nuclear Power Plants", published 1982, and reaffirmed 1998, should be considered:

- The reactor regulating system should be designed to maintain adequate effectiveness following credible single failures (clause 3.1 (c)) by meeting in general requirements in clauses 4.3.8.1 Reactivity Control Devices (which requires diversity of reactivity control devices such that failure of one set can be overcome by negative reactivity from another set), and 4.3.10 Response to Abnormal Events (which requires capability to sense abnormal events within the regulating system and elsewhere in the plant and to hold reactor power or reduce it at appropriate rates, setback and stepback actions).
- The system shall have available adequate negative reactivity to make and keep the reactor subcritical under all normal steady-state conditions and to prevent unwanted increase in reactor power, (Clause 4.3.13).
- The accident conditions, under which the system may be required to perform its role, shall include natural and man induced phenomena, as well as the cross-link effects of the pertinent initiating process failures to which the system must respond, (Clause 4.3.22.3).
- The reactor regulating system design shall incorporate features to keep fuel bundle and channel powers or rates of change, or both, below the limits of Clause 4.3.5.1.

5.2.5 Dose Acceptance Criteria/Dose Limits

A significant difference between the Pickering B licensing safety case and modern

requirements is in the approach to event categorization. The modern grouping of events into categories of AOO, DBA and BDBA is not done for Pickering B.

A list, Table 14 in reference 1, of AOO and DBA, based on the Pickering B Risk Assessment has been provided. Unfortunately, the list does not contain indications whether the listed events have been actually considered in the Safety Report, nor does it contain the predicted doses for the events. Furthermore, a number of events have not been shown to meet the AOO dose limits in S-310.

Some of the events have very high indicated frequency (especially in PRA event group # 13, 20.4, 21.1); one might think that a design modification could be justified to reduce the predicted failure frequency.

Specific comments on OPG's assessment are provided below:

- Appendix C.1.0 (p. 87): OPG is expected to compare the dose limits in S-310 of 0.5 mSv for AOOs and 20 mSv for DBAs to the doses listed in Sections C.1.2.2 and C.1.2.3. OPG then needs to determine the extent that the dose limits can be met through design and operational improvements.
- The pre-2004 dose limits listed in S-310 are not applicable for the purposes of the Integrated Safety Review. OPG stated in its' ISR Basis document [4] "*However, in order to determine the extent to which the plant meets the modern high-level safety goals and requirements, an assessment against the dose limits in the CNSC Draft Regulatory Standard S-310 Safety Analysis for Nuclear Power Plants for new NPPs shall also be performed.*", and CNSC staff expected OPG to compare against the S-310 dose limits listed above. Note, both Rem and mSv are used in this appendix, one set of units should be used to eliminate confusion.
- Section C.1.2.2: The actual predicted doses should also be listed in Tables 12 and 13. The data presentation in Tables 12 and 13 is misleading as it isn't clear what "Individual Dose Limit" is being considered. By inference from the text, it is apparent that the "% of Individual Dose Limit" is based on the dose limit in the Siting Guide (5 mSv for AOOs and 250 mSv for DBAs), so one needs to multiply the Siting Guide by the dose limit fraction (currently represented as a %) to obtain the predicted dose that needs to be compared against the S-310 dose limits.
- Section C.1.2.2: It is not clear why Items 5 and 7 are included in Table 12 if they are not in the AOO frequency range (p. 90). OPG needs to address this inconsistency.
- Section C.1.2.2: The discussion on Item 3 in Table 12, PT/CT Failure (in-core LOCA), is extremely difficult to follow. Two types of PT/CT failures are listed in the text on p. 90 and in Table 14 (these are PBRA event #'s 3.1 and 3.2 in Table 14); however, Table 12 discusses PT/CT failure with intact containment and blinded containment, and points to both PBRA event #'s 3.1 and 3.2. it is not clear which case (# 3.1 or # 3.2) is being considered for item #3 in Table 12. OPG needs

-
- to clarify this and indicate what design and/or operational changes could be implemented to reduce the dose from this type of event.
- Section C.1.2.2: Regarding Item 2 (End-fitting Failure, p. 90), the text provided is not adequate to support the recommendation of no further assessment of the item is needed. The analysis using better estimates of actual operating parameters, reducing analysis uncertainties and more realistic operator assumptions needs to be performed before this item can be considered as meeting the AOO dose limit. If re-analysis shows that end-fitting failure remains as an AOO, OPG needs to determine what design and operational changes can be implemented to reduce the consequences, or frequency, or both.
 - A design change option was briefly mentioned to address this issue (page 90). From the presented information it appears that no further consideration will be given to this design change; however, any suitable possibility to reduce doses to the public should be evaluated seriously;
 - Section C.1.2.2: Regarding item 4 (Fuelling Machine Induced Failure, p. 90), the text is extremely confusing. The event is classified as an AOO, and is listed as an AOO in both Tables 12 and 13. Yet, OPG provides a weak argument that because the PRA considers small LOCAs in the 100 – 1000 kg per second range as DBAs. OPG needs to provide adequate justification for Fuelling Machine Induced Failures as a DBA before OPGs conclusion regarding this item can be accepted.
 - Section C.1.2.4: Text on p. 91 indicates that PT/CT failure is not considered to be an AOO, yet in Table 14 PBRA event # 3.2 is classified as an AOO. Hence, the S-310 dose limit is not met for the PT/CT failure, and needs to indicate what design and/or operational improvements can be implemented to meet the S-310 dose limits. In addition, OPG needs to make significant clarifications to the text of Section C.1.2.4 (and Section C.1.2 in general).
 - Section C.1.2.3: OPG was expected to compare the dose limits in S-310 of 0.5 mSv for AOOs and 20 mSv for DBAs. The pre-2004 dose limits listed in S-310 are not applicable for the purposes of the Integrated Safety Review. OPG stated in its' ISR Basis document [4] "*However, in order to determine the extent to which the plant meets the modern high-level safety goals and requirements, an assessment against the dose limits in the CNSC Draft Regulatory Standard S-310 Safety Analysis for Nuclear Power Plants for new NPPs shall also be performed.*", and CNSC staff expected OPG to compare against the S-310 dose limits listed above.
 - Significant channel flow blockage (more than 90%) has an estimated frequency that puts this event into the AOO category; does the predicted dose meet the AOO dose limit?

5.2.6 Initiating Events

It is not clear that the set of initiating events considered is complete. It is a requirement of

a Periodic Safety Review to re-evaluate the initiating events taking into account the as-built plant and to do this using a systematic methodology such as failure mode, effect analysis, master logic diagrams. It appears that this was not done. OPG should not rely on past assessments of the range of possible initiating events but should perform a systematic determination.

Furthermore, the objectivity of the OPG review is questioned, for example, by the assigning “direct compliance” to NS-R-1 clause 2.7 (page 133) which requires that the safety analysis examines 1) normal operational modes; 2) AOO; 3) DBA and 4) BDBA. The current Pickering B deterministic analysis clearly does not cover all these categories of events. Similarly, compliance with clause 5.7 is judged to be “direct”, even though in it acknowledged that the current analysis does not consider events initiated by common cause or human errors.

In addition, Section D.1.5 states that the review whether C-006 initiating events are adequately addressed in Pickering B Safety Report was based on the existing review that was completed for Pickering A. It is not clear how such assessment for one plant can be based on an assessment for another plant having different design and Safety Report. OPG is requested to provide more details on the process they used for identifying initiating events.

Section 3.1.1.5.4, p. 26: OPG claims that all of the C-006 R1 events are adequately addressed in the Safety Report or are addressed in supplementary reviews including the Pickering B risk assessment, or in the Pickering A C-006 R1 review Initiating Event dispositions. Further, OPG claims that initiating events, event combinations and event combinations not covered by existing analyses are documented in Appendix F. However, CNSC staff note that Appendix F contradicts that text in Section 3.1.1.5.4 as information in Appendix F clearly indicates that some issues have not been addressed as yet. If there are outstanding issues regarding the completeness of the safety analysis, they should have been reported as discrepancies in the safety factor report, either in Table 4, section 4 or Appendix G.

Further to this, CNSC staff find the treatment of gaps (i.e., discrepancies) against the current licensing basis, and modern standards very confusing. CNSC staff expected that all discrepancies would have been listed Table 4, and that all outstanding issues in Appendices F and G are discrepancies that need to be addressed in the ISR.

Comments on Appendix F of the Safety Analysis Safety Factor report are provided below:

- Regarding Initiating Events, Item 2, Core By-pass due to Failure of ECCS Isolation Valves”: The Pickering “A” disposition states “This latter concern resulted in filling of SCR-P-2001-03725, and will be assessed in terms of trip effectiveness. This event is expected to not result in a serious process upset and to be bounded by pump trip events.” CNSC staff question whether the assessment was performed and request OPG to provide the supporting reference.

-
- Regarding Initiating Events, Item 4, End-fitting Failures: The second item discusses end fitting failures. The discussion given is not a complete consideration of all initiating events such a failed rolled joints or feeder pipe whip that lead to accident conditions.
 - Regarding Initiating Events, Item 5, “Plant response to a tornado”: Information provided by OPG in their disposition is inadequate. OPG states that “Qualitative assessment suggests that essential safety functions are expected to remain operable.” OPG is requested to provide the supporting documentation that demonstrates that essential safety functions will remain operable, and to fully describe what safety functions will remain operable. Although a frequency of 10^{-5} is low, it is still a design basis event, and needs to be assessed appropriately.
 - Regarding Event Sequences, Item 10, “Updating of Safety Analysis for LOCA plus loss of ECIS dual failure events”: OPG states that “The issue for Pickering B is that the current safety report is incomplete regarding LOECI coverage – Releases have not been assessed for small LOCA/LOECI, and Large LOCA. LOECI has not been presented in the current safety report”. This issue should have been listed as a **Discrepancy** with respect to modern standards in Table 4 of [1] and should have been clearly indicated as an issue in Appendix G of [1].
 - Regarding Event Sequences, Item 11, “Updating the Safety Analysis to Address Event Sequences involving credible impairments of either ECIS or NPCS in conjunction with a non-LOCA initiating event”: OPG indicates that this issue is to be addressed, yet it does not appear to be classified as a **Discrepancy** with respect to modern standards (i.e. listed in Table 4).
 - Regarding Items 10 and 11, it seems that in addition to being issues with respect to C-006 R1, there is an issue of non-compliance with the current licensing basis and is a **Discrepancy**. The Siting Guide requires dual failures such as those described in Items 10 and 11 to be addressed.
 - Regarding Event Sequences, Item 12, ““Single Line of Defence” Sequences”: OPG refers to a bulleted list, yet there is no bulleted list for Item 12. OPG is requested to clarify.

The text provided for the Pickering A disposition suggests that the analysis has not been performed, yet the text for the Pickering B assessment indicates that the work has been done. OPG states: “The issue for which further review is recommended relates to confirming that the safety impact is expected to be acceptable ...”, and OPG is requested to clarify the status of this issue.

In addition, OPG claims that the fourth bulleted item is dispositioned by availability of Group 2 provisions to cater powerhouse MSLB events”; however, it is noted that the limiting accident considered in the Pickering B Environmental Assessment is EPRC 5A, which involves releases following a powerhouse MSLB event. OPG needs to clarify the ability of provisions to cater to powerhouse MSLB events.

Additional comments on initiating events are:

- Page 221, NS-R-1 Clause 5.17, Aircraft Strike – While assessment for small aircraft strike event is addressed, the submission does not address the consequences of intentional large commercial aircraft crash or other similar malevolent actions [e.g. p. 220-225, p.243, etc.]. The conclusion of acceptable deviation is not supported. CNSC staff considers this issue should be classified as a **Discrepancy** in the ISR for disposition to determine corrective actions.
- Section C.1.2.4 states that "The protective provisions relating to containment all have demonstrable unavailability of $<10^{-3}$ yrs/yr. Hence, any initiating event with a frequency $<10^{-2}$ occ/yr would be in the Beyond Design Basis Accident category and would not be subject to the DBA dose limits." This statement is incorrect. The unavailability assessment of the containment, as it is performed currently by OPG, does not include reliability of support systems, common cause failures, human errors, etc. In other words, it does not reflect the probability that the containment would respond as expected when required to do so. Thus, this argument cannot be used in this context.

5.2.7 *Containment Performance*

Specific comments on containment performance are provided below:

- The safety factor report [1] fails to identify the need to assess containment performance for severe accidents and to consider design changes to manage severe accidents. The disposition of clause 4.11 of NS-R-1, as given in Appendix D Section D.2.1.1, is not considered to be meet the objectives of the requirement.

In particular, there are discrepancies in comparison with IAEA NS-R-1 Clause 5.31 or IAEA NS-G-1.2 Clauses 4.104 to 4.122 reported in Reference 1 (pg 189-191) related to severe accidents. IAEA NS-G-1.2 Clause 4.105 states, "The safety analysis should aim to quantify a plant safety margin and demonstrate that a degree of defence in depth is provided for beyond design basis accidents to severe accidents." OPG stated in Reference 1, "The analysis of containment challenges and potential failure modes needs to be reviewed in the light of more recent information, e.g., issues arising from the Severe Accident Management Guidelines (SAMG) work."

- Page 40, R-7 Clause 3.4.3. OPG identifies the safety analysis that shows that the structural integrity of containment will not be impaired to a degree that consequential damage to reactor systems could result is not current. OPG claim that although the current Pickering B Safety Analysis does not explicitly address this issue, a number of earlier assessments were performed that this can be considered "an acceptable deviation". CNSC does not concur with the classification as "an acceptable deviation", this should be classified as a **Discrepancy**. OPG has not demonstrated that the earlier stand-alone assessments for Pickering A remain valid for Pickering B according to current plant design,

configuration or condition (e.g. earlier assessments may not take into account ageing of concrete and reinforcement for life extension). Pickering B Safety Analysis should explicitly address this issue.

- Page 41, R-7 Clause 3.4.4. OPG identifies the safety analysis that demonstrates that all events specified in Tables 1, 2 and 3, will not damage the containment structure is considered to be out-of-date. OPG claim that although the current Pickering B Safety Analysis does not explicitly address this issue, a number of earlier standalone assessments were performed that this can be considered “an acceptable deviation”. CNSC does not concur with the classification as “an acceptable deviation”. OPG has stated that these stand-alone assessments are predominantly static documents that have not necessarily remained current with the plant design. OPG has not assessed that these stand-alone assessments remain valid according to current plant design, configuration or condition, or that they are valid for extended operating life, and current safety standards and operating experience. Therefore we consider this issue should be a **Discrepancy**.
- Section D.2.1.2: Regarding R-7, OPG has identified some “Acceptable Deviations”; however CNSC have a number of comments on OPG’s categorizations:
 - Clause 3.1: OPG states that “Although all failures have been addressed ... some of the assessments are not current”. This issue needs to be categorized as a **Discrepancy**, not an “Acceptable Deviation” since assessments are not current. The assessments need to be made current.
 - Clause 3.4.1: OPG states “In terms of break discharge, these assessments have not been revisited based on new safety analysis information, however, the results are expected to remain valid.” OPG needs to demonstrate that the results remain valid through updated assessments. Until assessments are updated, this issue is a **Discrepancy**
 - Clause 3.4.2: OPG states “The current Pickering B safety analysis does not explicitly address negative design pressures. Are expected to remain valid.” As above, OPG needs to demonstrate that the results remain valid through updated assessments. Until assessments are updated, this issue is a **Discrepancy**.
 - Clause 3.4.4: OPG states “While the current Pickering B safety analysis does not ... are expected to remain valid.” As above, OPG needs to demonstrate that the results remain valid through updated assessments. Until assessments are updated, this issue is a **Discrepancy**.
 - IAEA NS-G-1.2 Clause 4.115, p. 192: OPG states “... the analysis of containment challenges and potential failure modes needs to be modeled without this accuracy being quantified. However, it is expected that modeling of various components will be sufficiently accurate.” OPG indicates that modeling is needed, and on the other hand suggests that the modeling will be accurate. This issue needs to remain a **Discrepancy** until the modeling is completed.

5.2.8 System Performance Issues

CNSC staff have the following comments regarding safety analysis aspects of specific systems:

- Executive Summary, p. 6, 3rd paragraph: It is stated that the rigorous process of developing the SOE resulted in the identification and reconciliation of many issues (gaps) in the safety analysis area. Recently, CNSC staff reviewed the OSR of service water system and had a number of safety concerns [6]. OPG needs to provide proper disposition for all the safety concerns.
- OPG has not considered the following safety analysis issues that were identified in reference [7]:
 - Timing issues for Group-2 systems;
 - Adequacy of 15 minutes to energise all Class-III busbars, during the worst case scenario of only one standby generator feeding two units (LOBES);
 - Operability of motorised valves during degraded voltage condition;
 - Adequacy of battery testing;
 - QA issues with ETAP program.
- Hazard Analysis, Section 3.1.3: OPG has not considered the absence of fire water for 15 minutes during one standby generator feeding two units (during LOBES scenario) [8].
- Section 3.1.3.5.2, p. 62: It is stated that potential issues to be considered include EWS booster pump operation. CNSC staff were informed during the Type 1 electrical system functional inspection that there is no requirement for EWS booster pumps. Why OPG is reconsidering EWS booster pump operation? Please clarify.
- The first row on page 35 discusses compliance with the single failure criteria in special safety systems or support systems. The issue is considered to be an acceptable deviation by OPG based on the facts that instances of no redundancy in systems important to safety are addressed with high priority per the impairment procedures, and that in CANDU design the approach has been to ensure that there are alternate functions available to mitigate accidents rather than to have multiple system trains that perform the same function.

The first argument is questionable and should not be accepted by CNSC. All reasonable measures shall be taken by OPG to eliminate singletons in systems important to safety. The second argument is acceptable; however, OPG needs to perform a systematic assessment of all existing singletons to make sure that for every such instance there exist a back up safety function. For instance, OPG can keep one of EPG in maintenance for several weeks while two EPGs is the only power supply source for mitigation of common mode events. Thus, any single failure in so complex equipment as EPG during mitigation of an accident would disable all safety functions.

CNSC staff believes that this issue is a **Discrepancy** and OPG needs to perform a systematic analysis and all reasonable design modifications to eliminate all singletons in systems important to safety.

It is concluded that there is a deviation in the application of single failure criterion as required by modern standards (page 151). This may have a significant effect on the demonstration of effectiveness of defense in depth. Nevertheless, no consideration is given to either modifying the design or the analysis. Alternatively, it should be demonstrated by assessments that the implemented approach is equivalent in its safety implications.

5.2.9 *Pickering B Risk Assessment*

CNSC staff have the following comments regarding the Pickering B Risk Assessment:

- Item 9 on page 114 states that "The PBRA addresses both at power and shutdown states." Based on CNSC staff review of the PBRA, CNSC staff concludes that there are significant deficiencies in the methodology. CNSC staff will track this issue under compliance with S-294 and expect that all concerns will be addressed.
- The first paragraph on page 50 claims that internal floods are modeled in the PBRA. Based on CNSC staff review of PBRA revision 1, CNSC staff concludes that no comprehensive flood assessment has been performed; only consequential floods have been considered. Thus, CNSC staff request a comprehensive flood assessment for Pickering B. This needs to be identified as a **Discrepancy**.
- Page 53, S-294 Clause 5.8 (also NS-R-1 Clause 5.73). OPG identifies the PBRA does not currently contain risk contributors from fire or external events such as seismic and tornado initiators. We agree with the OPG classification of this issue as a **Discrepancy**. OPG claim they have addressed these events via hazard assessments and design (i.e. fire and seismic). However to substantiate this claim, OPG should:
 - List the postulated imitating events (PIE) that are not covered by the PBRA,
 - Identify the specific assessments that address the PIE not included in the PBRA; and whether any assessments are missing.
 - Assess whether the assessments are valid and adequately address the PIE for intent of S-294 or NS-R-1.
- Page 53, S-294 Clause 5.8 (also NS-R-1 Clause 5.73). Further to the previous comment that the PBRA does not currently contain risk contributors from fire or external events such as seismic and tornado initiators. OPG states on page 64, "The international experience with PSAs of nuclear power plants shows that the risk derived from external events can be a significant contributor to core damage frequency in some instances".

CNSC staff considers that the PBRA should include fire, turbine generator missile, and external events such as flooding, tornado and seismic event initiators, to

understand the risk contribution of these events to the core damage frequency.

- Section C.3.5, p. 115, “10 *Include sensitivity analysis, uncertainty analysis and importance measures in the PRA.*” The absence of CNSC or industry guidance is not adequate to justify this issue as an “Acceptable Deviation”. It is a **Discrepancy** and OPG needs to include sensitivity analysis, uncertainty analysis and importance measures in the PRA. OPG needs to indicate when these analyses will be performed.

5.2.10 *Hazard Analysis*

CNSC staff comments regarding hazard analysis are provided below:

- Reference 1 (Section 3.1.3) states, “A thorough review of hazard assessments was completed and is documented in this report. In addition, the same assessment contains clause-by-clause reviews of IAEA NS-R-1, Regulatory Documents R-7, R-8 and R-9, and CSA Standard N290.6. These documents have a number of clauses that are applicable to ‘Hazard Analysis’. These reviews are considered to fully satisfy the objective of this safety factor.”
However, a hazards analysis methodology has different acceptance criteria and different analysis methodologies than Deterministic Safety or Probabilistic Safety Analyses. Therefore, it is not evident how the list of documents given in Section 3.1.3.2.1 applies. As well, the process described in Section 3.1.3 does not provide for an actual review of the hazards. For example, changes in weather patterns may invalidate older studies of wind and flooding hazards? Some of the hazards analyses appear to be out of date and so need re-assessment.
- CSA N293-95 has been revised and the current version, CSA N293-2007 has been published. CNSC staff consider the requirements and guidance provided in the revised standard as applicable to an ISR assessment and recommend that OPG should be requested to revise their assessment against the revised version in their Emerging Issues process. It should be noted that in the revised edition, issues such as fire and explosion related deterministic hazard analysis was substantially revised and reflect modern approaches.
- CNSC staff does not concur that the existing governance addresses FHA / FSSA maintenance and therefore ensures the adequacy of hazard analysis with respect to fire and compliance with the PROL. The FHA and FSSA do not reflect current configurations in the field, maintenance and updates are not governed under document maintenance procedures and maintenance requirements are not addressed in the fire protection program. As identified in the fire protection program review performed by CNSC staff [9], and confirmed via discussions with OPG, the FHA and FSSA maintenance and updates are not governed under document maintenance procedures and maintenance requirements are not addressed in the fire protection program. CNSC staff considers this issue should be classified as a **Discrepancy** in the ISR for disposition to determine corrective actions.

-
- The FHA and FSSA are limited to 100% power operation and do not address other plant states, notably shutdown. The existing governance does not address this requirement. This should result in the Direct Compliance conclusions on p. 128 being changed from Direct Compliance to.
 - OPG recognizes that the magnitude and frequency of the seismic hazard spectra impacts on the qualification of the Systems, Structures, and Components and that if their required qualification were to change, the success path may need also to change. OPG claims there is no evidence of any additional information or insight in terms of quantification of the seismic hazard that would invalidate Pickering B's safety case for seismic events. Notwithstanding, the fact that there remains some ongoing activities in terms of establishing seismic hazard uncertainties, OPG assesses this results in the level of compliance as being an Acceptable Deviation. OPG concludes the issue of seismic hazard uncertainty is not expected to impact on the seismic safety case for Pickering B life extension. However, it is recommended that issues relating to the Building Code spectra and the Pickering A RLE spectra should be reconciled and documented in the Pickering B seismic safety case. CNSC staff considers this issue should be classified as a **Discrepancy** in the ISR for disposition to determine corrective actions.
Specific comments are:
 - OPG concludes the issue of seismic hazard uncertainty is not expected to impact on the seismic safety case for Pickering B life extension. However there is no technical basis provided in the report to support the conclusion of this statement.
 - OPG claimed that there is no evidence of any additional information or insight in terms of quantification of the seismic hazard that would invalidate Pickering B's safety case for seismic events. The statement seems to contradict the fact that the recently published National Building Code of Canada (NBCC) 2005 provides additional information in the quantification of the seismic hazard across Canada.
 - In CSA N289.2, design ground response spectrum is defined as "the response spectrum developed from the design basis seismic ground motion (DBSGM) or the site design seismic ground motion (SDSGM)". Furthermore in CSA N289.2, design basis seismic ground motion is defined as "the seismic ground motion at the site that represents the potentially severe effects of earthquakes in the region and that has a sufficiently low probability of being exceeded during the lifetime of the plant...". There is no technical basis, such as a seismic hazard assessment, provided in the report to demonstrate that the existing design basis earthquake ground response spectra used in Pickering B plant design represent potentially severe effects of earthquakes in the region and has a sufficiently low probability of being exceeded during the extended service life under the Pickering B refurbishment project.
 - Similar to the above comment, the design basis earthquake (DBE) used in the original design of the Pickering B plant is 5%g (i.e. 0.05g) peak horizontal acceleration according to Refs. [10, 11]. Does this peak

horizontal acceleration have a sufficiently low probability of being exceeded during the lifetime of the plant?

- Page 59, Section 3.1.3.3, Common Mode Events SDMs. The ISR report states “In general, the original design basis treatment of natural events was in development of the original Pickering B safety design matrices (SDM) to assess floods, earthquakes, etc. (References [R-18], [R-19], and [R-20] in the Safety Factor Report [1]), as there is no analysis of earthquake presented in the Safety Report analysis section....This continues in the current Pickering B Safety Report and Risk Assessment (PBRA), neither of which includes design basis earthquake. The Pickering B Seismic SDM study for operation after an earthquake (Reference [R-18]) remains as the key design basis document for seismic events”.

The referenced SDM documents [R-18, R-19, R-20] all date from 1981. OPG has not assessed that the SDMs remain valid according to current plant design, configuration or condition, or that they are valid for extended operating life, and current safety standards and operating experience. Therefore we consider this issue should be a **Discrepancy**.

- Page 59, Section 3.1.3.3, Fire Hazards. CNSC staff does not concur that the existing governance address Fire Hazard Assessment (FHA) maintenance and therefore compliance. As identified in CNSC staffs fire protection program review (Ref. 4) and confirmed via discussions with OPG, the FHA and FSSA maintenance and updates are not governed under document maintenance procedures and maintenance requirements are not addressed in the fire protection program. The Fire Hazard Assessment (FHA) [and the resulting Fire Safe Shutdown Analysis (FSSA)] and Code Compliance Review have not been maintained to reflect current field configuration. The code compliance review was a voluntary assessment that the station undertook to identify and disposition life safety issues which revision is currently not enforceable via license requirements. However, the Fire Hazard Assessment is required to reflect the current plant configuration (as per the CSA N293-95 edition) and therefore this result in a **Discrepancy**.
- Page 59, Section 3.1.3.3 states “Pipe ruptures in Pickering NGS B have been studied extensively to assess their potential for further damage to other components which could jeopardize the safe shutdown and continued cooling of the reactor (References [R-31], [R-32], [R-33], [R-34] and [R-35]). These studies considered the effect of pipe whip and jet effects. The layout was reviewed to ensure that loop-to-loop break propagation would not occur”.

References [R-31], [R-32], [R-33], [R-34] date from the mid 1970's to early 1980's while [R-35] dates from 1990. There has been considerable evolution in the requirements and technologies for prevention and consequences of pipe rupture. OPG has not assessed that these early assessments remain valid according to current plant design, configuration or condition or that they are valid for extended operating life, and current safety standards and operating experience”. Therefore CNSC staff considers this issue should be classified as a **Discrepancy** in the ISR

for disposition to determine corrective actions.

- Page 62, Section 3.1.3.5.2, states “Although there is a seismic safety case at Pickering B, the SDM that established the success path for Pickering B was issued in 1981 and has not consolidated more recent developments relating to the seismic safety case (i.e., the work is fragmented, refer to SCR P-2000-01917). Potential issues that may need to be consolidated include: a) HTS heat-up, b) bleed condenser level control valve seismic override, c) 1” HTS equivalent hole size, d) EWST make-up, e) CCAFF, f) fire protection, g) EWS booster pump operation, h) reconciliation with the SMA Building Code, i) instrument air requirements, j) use of seismic monitoring instrumentation, k) operator action time credit, l) implicit credit for Loss of Class IV (LOCLIV) Power, m) turbine generator protection, and n) HTS valve leakage”. CNSC staff considers this issue should be classified as a **Discrepancy** in the ISR for disposition to determine corrective actions.
- Page 62, Section 3.1.3.5.2, states “In addition there are various seismic related issues present at Pickering B relating to the Peak Ground Acceleration (PGA) assumed in the design basis of the plant, seismic qualification of the SDS1, HPECI and fire protection systems at Pickering NGS B”. CNSC staff considers this issue should be classified as a **Discrepancy** in the ISR for disposition to determine corrective actions.
- Page 62, Section 3.1.3.5.2, states “previous assessments of the potential for external flooding at the Pickering NGS A site may need to be reviewed for applicability to Pickering B.”. CNSC staff considers this issue should be classified as a **Discrepancy** in the ISR for disposition to determine corrective actions.

5.2.11 Quality of the Safety Factor Report

In general, the report follows requirements of the ISR Basis document. Every review element from the ISR Basis Document has a separate review section in the report. Many reviews performed in this report are correct and identify existing issues as discrepancies for further resolution during the definition of refurbishment scope. However, CNSC staff disagree with a number of dispositions of deviations/discrepancies in which OPG states their position without substantiation, or make conclusions without confirmation.

Specific comments on categorization of findings by OPG are provided below (as well as those provided in Sections 5.2.1 through 5.2.10 of this report):

- The first row on page 38 states "This clause requires that process failures 1-7 (LOCAs and losses of HTS inventory) be addressed in conjunction with a coincidental impairment of ECI. All failures have been addressed in supplementary assessments." However, no reference is provided to these assessments.

-
- In comparison with R-7, the safety analysis supporting the maximum negative design pressure of the containment is considered an acceptable deviation for the reason that new analysis using GOTHIC has not been performed but conclusions from the earlier assessments are expected to be valid? Comments on page 39 state that "The current Pickering B Safety analysis does not explicitly address negative design pressure. Although new analysis using GOTHIC has not been performed, the conclusions from these earlier assessments are expected to remain valid." The basis for this conclusion is unclear. OPG has to explain how it is supported.
 - A requirement of R-7 is that the safety analysis should show that the structural integrity of containment will not be impaired to a degree that consequential damage to reactor systems could result. For this, OPG refers to the earlier analysis in support of LOCA + loss of shutdown in D&D Report #87428 "Pickering GS A Concrete Containment Structural Response and Assessment of Failure Thresholds". It is not clear that the basis for that analysis and the results of this analysis continue to be valid, and no assessment of this aspect is reported.
 - Executive Summary, p. 6: It is acknowledged that CSA N286.7 does permit use of legacy codes that have not undergone complete verification and validation. In addition, OPG is correct in stating that gap assessments are needed to show that analysis remain conservative. However, this issue is not an "Acceptable Deviation". Instead it is a **Discrepancy**, as it is a gap with respect to modern standards (specifically IAEA NS-R-1, Clause 5.70, OPG states in [1]).
 - IAEA NS-R-1 Clause 5.70 and NS-G-1.2 Clauses 4.86, 4.87, 4.88, p. 156 and p. 157: OPG has provided appropriate text with regards to the status of computer codes; however, the two issues are to be categorized as a **Discrepancies** rather than as "Acceptable Deviations". OPG needs to provide their plan for performing safety analysis with appropriately validated codes.
 - Section 3.1.1.3, p. 19: OPG states that "the reviews conducted in Appendix D of this report did not identify any discrepancies relation to quality management." However, as indicated in comment #1, OPG acknowledges that there are issues with respect to code validation and, as such, is a **Discrepancy**.
 - Section 3.1.1.5.3, p. 23 and Appendix C2.0: OPG states that their review of CNSC regulatory document G-144 identified five clauses that were Acceptable Deviations relating to trip windows, fuel post-dry-out operation and the 600 C/60 s requirements, and the interpretation of the acceptance criteria relation to acceptable duration of post dry-out operation. OPG has not provided adequate information to support their categorization of these clauses as Acceptable Deviations.

The issue of compliance with G-144 requirements is largely based on the CNSC position regarding the adequacy of the existing fuel bundle design test database. Furthermore, on p. 101, OPG states that they are in Direct Compliance with Section 2 of G-144. They state: "OPG is currently undertaking experiments at Stern

Laboratories, though COG WP 20905, to collect full-scale Post Dryout data for 28 element fuel bundles. This will provide definitive evidence on PDO heat transfer analysis and hence Pickering B will be in compliance in the clause related to PDO data.”

However, this must be considered as a **Discrepancy** as the results from the experimental program referred to by OPG have indicated that is not in compliance with the clause related to PDO data. OPG submitted an S-99 report on the unanticipated findings in June 2007; however, the unanticipated findings were obtained from tests completed in the spring 2006.

Furthermore, with respect to G-144, OPG found it appropriate to dedicate substantial effort to arguing against the premises of G-144 (e.g., on pages 105-107). The ISR report is not the appropriate place to challenge this regulatory document.

- Section 4 and Appendix G: Section 4 is titled “Review of Licensing Issues”; however it is not clear that it only applies to Appendix G of the report. Instead this section should have provided a summary of all licensing issues, and all discrepancies and acceptable deviations identified in the report (i.e., a summary of Tables 4, 6 and 7, and Appendices F and G). Furthermore, in the Executive Summary (p.7), OPG indicates that there are 12 Pickering B specific discrepancies against modern codes and standards; however Appendix G lists numerous Safety Analysis deficiencies. CNSC staff expect that this list of issues will be addressed by OPG.

Specific comments on Appendix G are provided below:

- OPG needs to better explain why the issues listed in Appendix G are the issues that are focused on out of the 680 items.
 - Compared to Section 4, the information in Appendix G appears to be incomplete. Section 4 indicates that there are 67 low risk issues, yet Appendix G only contains 31 low risk issues. Furthermore, OPG does not list, nor discuss, the following: “Open – Resolution Plan Pending”, “Resolution Plan in Place”, and “Program Requirement”. Clearly these are issues that need to be addressed in the ISR – having a resolution plan in place does not mean the issue is addressed, the issue remains as a **Discrepancy** until the resolution plan is completed and implemented.
 - The text accompanying each issue is inadequate to describe the issue, and its status.
 - Some issues, such as #106, #108, #142 and #233, are of concern and need to be addressed in a timely manner.
- Comments on Summary of Findings from Deterministic Safety Analysis Review (Table 4, p. 33)
 - Compliance with NS-R-1:
 - for “Ability for reactor to shutdown for AOOs ...”, the Compliance category is listed as **Discrepancy** whereas the accompanying text states

-
- that it is an acceptable deviation. OPG is requested to clarify the categorization;
- the justification provided for the post-LOCA hydrogen ignition system is not adequate to support its categorization as an Acceptable Deviation. The issue is clearly a **Discrepancy**, and based on meetings in July 2007, OPG has committed to install PARS as a condition for close-out of GAI 88 G02;
 - Regarding the issue “some of the assessments that demonstrate that structures ... of the safety analysis”, the justification that some reports done outside of the Safety Report is part of the licensing basis is acceptable. However, these “stand-alone” assessments will be captured in the updated Safety Report that OPG and the industry has committed to do.
 - Compliance with R-8:
 - Regarding “The annunciators and ... the safety analysis”, that a review is underway is not adequate to support categorization as an “Acceptable Deviation”. The issue remains a **Discrepancy** until it is resolved via a design change, operational considerations, or sufficiently supported analysis.
 - Regarding single parameter trip coverage, the issue is to be considered as a **Discrepancy** unless adequate justification has been provided, or references provided indicating CNSC acceptance of the cases where there single parameter trip coverage. OPG should revisit these situations and determine whether design improvements are possible at the time of the life extension outage.
- Comments on Table 6, Summary of Findings from Review of Probabilistic Safety Analysis Review:
 - Regarding “Uncertainties relating to monitoring hydrogen concentration in containment for severe accidents”: OPG categorizes the issue as an “Acceptable Deviation”; however, OPG needs to provide the reference to the information on the approach they have adopted for monitoring hydrogen following a severe accident.
 - Regarding the item “SDS1 not fully seismically qualified” in table 7 (p. 66), since SDS1 is not fully seismically qualified, and does not meet the clause in R-8, this issue needs to be categorized as a **Discrepancy** (although the Design Guide permits the configuration). OPG should consider means to fully seismically qualify SDS1.
 - IAEA NS-R-1 Clause 6.64, R-7 Clause 3.10.2, IAEA NS-R-1 Clause 6.44, IAEA NS-R-1 Clause 6.46, IAEA NS-R-1 Clause 6.66, p. 164, p. 178, p. 201, p. 202, p. 204: OPG categorizes these issues as “Acceptable Deviations” or “Direct Compliance”, but given that the PLHIS is available for hydrogen mitigation in the short term following a LOCA + LOECI, OPG needs to implement design changes to address long-term hydrogen management. All issues should be categorized as “Discrepancies”.

-
- IAEA NS-R-1, Clause 5.41, p. 194: OPG categorizes this issue as an “Acceptable Deviation”; however, until the reliability models are developed, this issue should be categorized as a **Discrepancy**.
 - The conclusion reached by OPG in assessing compliance with NS-R-1 Clause 6.9 is unsupported. Clause 6.9 requires that in design basis accidents, the fuel elements ... shall not suffer distortion to an extent that would render post accident cooling insufficiently effective. OPG finds that there is direct compliance with this requirement, even though for several events (single channel stagnation break, flow blockage) this requirement cannot be met; the current Large Break LOCA analysis cannot rule out significant fuel geometry distortion.
 - IAEA NS-R-1 II.5, p. 206: A far more detailed discussion of Common Cause Failures is required to support the claim of Direct Compliance with this clause.
 - IAEA NS-G-1.2, Clause 3.82, p. 233-234: OPG states “A similar review of the use of non-diverse components on SDS1 and SDS2 should be conducted to confirm that there are no common mode failures that could impact on both system’s unavailabilities and invalidate failure to shutdown assumptions...”. OPG then states “This issue is considered and Acceptable Deviation ...and of high quality.” This is a significant issue and since there are non-diverse components, the issue needs to remain a **Discrepancy** until the review and analysis is completed.
 - N289.1-80, p. 256-257: OPG states “Although the reliability model for RRS may be out of-date functional and performance requirements.” That the RRS has operated effectively for many years is not adequate justification to support it’s categorization as an “Acceptable Deviation”. The issue needs to be categorized as a **Discrepancy** until the reliability model is updated.

5.3. Conclusion

OPG undertook a review of the Safety Analysis subject area as part of the integrated safety review for the planned Pickering B plant life extension project. The OPG report on Safety Analysis subject area includes three safety factors: deterministic safety analysis probabilistic safety analysis and hazard analysis. The objectives of the OPG review were to determine, within this subject area:

- the extent to which the plant conforms to modern requirements;
- the extent to which the licensing basis remains valid in terms of meeting the current regulatory requirements; and
- the effectiveness of arrangements to maintain plant safety for long-term operation.

For deterministic analysis specifically, OPG aimed to confirm that:

- the current analysis takes into account the actual plant design;

- the analysis covers the conditions of plant at the end of plant life; and
- current knowledge, methods and standards are incorporated in analysis.

CNSC staff provided comments with respect to:

- Completeness and Comprehensiveness of the Safety Report
- Fuel and Reactor Core Nuclear Design
- Shutdown System Effectiveness
- Reactor Regulating System
- Dose Acceptance Criteria/Dose Limits
- Initiating Events
- Containment Performance
- System Performance Issues
- Pickering B Risk Assessment
- Hazard Analysis
- Quality of the Safety Factor Report

CNSC staff conclude that:

- It is concluded that the safety analysis safety factor report is incomplete and requires further work. This should involve not only addressing the CNSC staff's findings adequately, but also involve additional safety analysis and, to the extent practicable, implement design and operations modifications to address all identified shortcomings.
- The information on fuel and reactor core nuclear design in Safety Analysis Report and supporting references is fragmented, incomplete, and the values of key basic nuclear parameters are based on obsolete information and neutronic methods and computer codes which are no longer supported by OPG.
- The impact of fuel and reactor core design parameters which are different from values at the time of original licensing on design control parameters for control and safety systems has not been discussed in reference 1.
- The existing outstanding safety issues related to effectiveness of shutdown systems have not been discussed in OPG assessment. Among the most significant outstanding issues are:
 - SDS1 reactivity depth
 - Shutdown systems effectiveness for reactivity and power mismatch transients
 - Shutdown systems effectiveness and large LOCA safety margins
- There has been no systematic analysis of the capability of the control system to cope with AOOs as required by modern standards.
- We cannot confirm OPG conclusion that the deterministic analysis as it is documented in the current Safety Report is conformant to the modern codes and standards. This is because:

-
- a significant part of the analyses in the Safety report was performed with computer codes which were not demonstrated to be applicable, e.g., validated, verified, subjected to quality control or properly documented.
 - some analyses, performed at the time of original licensing do not consider effects of design modifications, plant aging or changes in operating limits and conditions.
 - some of the initiating events, which should be considered according to the modern requirements, have not been analyzed. This includes whole categories of events such as beyond design basis accidents, as well as accidents initiated by human errors, and external and internal common cause events.
 - there exists a long list of outstanding issues (about 200 issues categorized in Section 4; some are described in Appendix G of Reference 1) with many elements pertaining to the current safety analysis.
 - for several events in the current Safety Report it was not possible to demonstrate compliance with radiation dose limits in modern standards.
 - application in safety analysis of the single failure criterion is not rigorous and is not in conformance to the modern requirements.
 - OPG's assessment of deterministic safety analysis area is incomplete and lacks adequate depth. The deterministic safety analysis for Pickering B refurbishment needs to be carried out anew using the modern day knowledge, actual description of Pickering B fuel and reactor core nuclear design, feedback from operating experience, state of the art models and computer codes, generally accepted standards and best practices. This can be done as part of RD-310 implementation.
- The safety factor report [1] fails to identify the need to assess containment performance for severe accidents and to consider design changes to manage severe accidents.
 - CNSC staff considers that the PBRA should include fire, turbine generator missile, and external events such as flooding, tornado and seismic event initiators, to understand the risk contribution of these events to the core damage frequency. CNSC staff notes that the PBRA does not address fire in operation or shutdown and therefore the contribution from fire to the shutdown PSA is not addressed.
 - Several discrepancies have been noted with regards to hazard analysis. In particular, issues regarding Fire Hazard Assessment (FHA) and the resulting Fire Safe Shutdown Analysis (FSSA), seismic qualification and its accompanying safety assessment, pipe rupture and flooding.
 - Many reviews performed in this report are correct and identify existing issues as discrepancies for further resolution during the definition of refurbishment scope. However, CNSC staff disagree with a number of dispositions of direct compliances and acceptable deviations in which OPG states their position without substantiation, or make conclusions without confirmation.

- Final conclusions on the adequacy of Safety Analysis will not be made until the Safety Factor report on the Actual Condition of SSCs is reviewed, the review of the Plant Design Safety Factor report [5] has been completed, and those results considered in the review of the Safety Analysis Safety Factor report.

5.4 References

1. Ontario Power Generation Report, "Pickering NGS-B Integrated Safety Review – Safety Analysis Review", June 29, 2007, NK30-REP-03680-00005-R000, CNSC File No. 26-1-8-1-8.
2. Ontario Power Generation, "NGD Integrated Safety Reviews", N-PROC-LE-0001, July 2007.
3. International Atomic Energy Agency Safety Guide No. NS-G-2.10, "Periodic Safety Review of Nuclear Power Plants", Vienna, 2003.
4. Ontario Power Generation, "NGD Integrated Safety Reviews", N-PROC-LE-0001, July 2007.
5. Ontario Power Generation Report, "Pickering NGS-B Integrated Safety Review – Plant Design Safety Factor", August 22, 2007, NK30-REP-03680-00001-R000, CNSC File No. 26-1-8-1-8.
6. Letter from K. Ramaswamy, P. Wan, G. Cherkas, "Review of Pickering-B Operational Safety Requirements (OSR) Service Water System", May 17, 2005, BITS # 968527.
7. CNSC Type-1 Electrical System Functional Inspection Report, December 15, 2006, BITS # 1085511.
8. Letter, G. Cherkas to K. Ramaswamy, "Water Supply for Fire Protection at Pickering Nuclear Generating Station-B ", February 14, 2006, BITS # 1145596.
9. Bounagui, A., to Bélanger, P., "Ontario Power Generation Darlington NGS – Fire Protection Program Review, BITS 3033520, Task 9563", dated 09 August 2007, File 26-1-13-4-2, BITS 3069314.
10. Letter, D. Patrick McNeil to T. E. Schaubel, "Pickering NGS-B - Integrated Safety Review – Safety Analysis Safety Factor Reports", June 29, 2007.
11. Letter, D. Patrick McNeil to T. E. Schaubel, "Pickering NGS-B- Integrated Safety Review Basis Document (Revision 1)", December 20, 2007, Bits 1379590.

APPENDIX 1

Reactor Core Design

It is expected that OPG will carry out a condition assessment and reconstitution of the reactor core nuclear design. These are expected to provide detailed information in the following areas, to allow an adequate review and assessment of the extent of conformance with modern standards and adequacy of design provisions:

1. Confirmation that nuclear design bases are established as required by the appropriate CNSC regulatory design requirements.
2. The reactor core incorporates inherent and/or passive safety features having a significant bearing on the probability or consequences of accidental release of radioactive materials.
3. Description of the design defence in depth capabilities for reactivity control safety function for each level of defence. The description should include a comprehensive inventory of all the challenges and mechanisms which may impact on intended performance of safety functions, and identify design safety provisions for achieving the objectives of each level of defence. The description should identify all design provisions ensuring performance of the following safety functions:
 - To prevent unacceptable reactivity transients;
 - To shut down the reactor as necessary to prevent AOOs from leading to DBAs and to shut down the reactor to mitigate the consequences of DBAs
 - To maintain the reactor in a safe shutdown condition after all shutdown actions;
4. The standards used conform to the generally accepted modern engineering standards applied to the design of the nuclear reactors.
5. Full description and supporting information of design core power distribution, including the following:
 - The design expected power distributions including normal and extreme cases for steady-state and allowed power maneuvering transients and covering a full range of reactor conditions during reactor operating life-time, allowed reactivity devices configurations, and possible fuel burnup distributions.
 - The design core power distributions as axial, radial, and local distributions and peaking factors to be used in the transient and accident analyses. Power distributions within fuel pins are also required. The phenomena and their effects should be identified and included in these distributions and factors.
 - The breakdown of design power distributions into power generated in the fuel (fission power), power transferred to the coolant (thermal power), power transferred to the core internals, and gamma heating.

- The conversion of the design power distributions into operating power distributions, including instrument-calculation correlations; operating procedures and measurements; and necessary limits on these operations.
 - The requirements for instruments, the calibration and calculations involved in their use, and the uncertainties involved in conversion of instrument readings into power distributions.
 - Limits and setpoints for actions, alarms, or automatic trip for the instrument systems and demonstration that these systems can maintain the reactor within design power distribution limits.
 - Measurements in power reactors and critical experiments and their use in the uncertainty analyses and the planned measurements to be made, including startup confirmatory tests and periodically required measurements.
 - The conversion of design limits, uncertainties, operating limits, instrument requirements, and setpoints into operating limits and conditions.
6. Full description of reactivity coefficients, including supporting analytical and experimental information. Specifically, the following should be covered:
- Calculated nominal values for the reactor core reactivity coefficients. The range of reactor states to be covered should include the entire operating range from cold shutdown through full power and the extremes reached in transient and accident analyses. It should include the extremes of fresh core, pre-equilibrium core, and burnup distributions in equilibrium core and an appropriate range of reactivity devices configurations for the reactor states. It should be demonstrated that the coefficients used are conservative. The information on reactivity coefficients should cover the full applicable range of the variables and modeling approximations in transient and accident analyses, including approximations related to modeling and nodalization of reactor core and cooling system.
 - Uncertainty analyses for nominal values, including the magnitude of the uncertainty and the justification of the magnitude by examination of the accuracy of the methods used in calculations, and comparison where possible with reactor experiments. For comparisons to experiments, it is important to show that the experiments are applicable and relevant.
 - Combination of nominal values and uncertainties to provide suitably conservative values for use in reactor steady-state analysis (primarily control requirements), stability analyses, and the transient and accident analyses.
7. Full description of reactivity control requirements and control provisions. It should include:
- The control requirements and provisions for control necessary to compensate for long-term reactivity changes of the core, including reactivity changes due to depletion of the fissile material in the fuel, and buildup of fission products and transuranic isotopes.

- The control requirements and provisions for control needed to compensate for the reactivity change caused by changing the temperature of the reactor from the hot zero power condition to the cold shutdown condition.
 - The control requirements and provisions for control needed to compensate for the reactivity effects caused by changing the reactor power level from full power to zero power.
 - The control requirements and provisions at various times during the refueling.
 - The control requirements and provisions for control needed to compensate for the effects on the power distribution and stability of the high cross-section neutron capture of the fission product nuclide xenon-135.
 - The adequacy of the control systems to assure prevention of anticipated reactivity transients to escalate to transients requiring action of shutdown systems.
 - Discussion of shutdown margins. Shutdown margins need to be demonstrated for all permitted operating states throughout the entire expected operating lifetime.
 - Uncertainties associated with the reactivity devices needs to be considered, including:
 - Manufacturing tolerances
 - Methods errors
 - Operation other than planned
 - Depletion
 - Measurement uncertainty in shutdown margin demonstration
8. Full description of expected and allowed reactivity devices configurations and reactivity worths. It should include:
- Descriptions and figures indicating the reactivity devices configurations expected for all permitted operating states throughout operating expected lifetime, power manoeuvring, and load following where applicable. It should include operation of single rods or banks of rods, withdrawal order, and insertion limits as a function of power and core state.
 - Descriptions of allowable deviations, such as for misaligned rods, stuck rods, if any.
 - Descriptions, tables, and figures of the maximum worths of individual reactivity devices and banks as a function of position for operating conditions appropriate to rod withdrawal transients, LZC draining transients and other conceivable failures of reactivity control components leading to positive reactivity insertions. Descriptions and curves of maximum rates of reactivity increase associated with reactivity devices withdrawals and any other conceivable change in configuration of reactivity devices due to failures in reactivity control system, experimental confirmation of rod worths or other factors justifying the reactivity increase rates used in safety analyses, and equipment, administrative procedures, and alarms which may be employed to restrict potential reactivity insertion should be included.

- Descriptions and graphs of trip rundown reactivity as a function of time after trip initiation and other pertinent parameters, including methods for calculating the rundown reactivity.
9. Discussion and predictions giving the values of core excess reactivity, maximum local powers, amount of fuel loaded per refueling operation, and frequency of refueling load should be included. Description of the basis for assuming that the maximum core excess reactivity and predicted local power peaks will not exceed the control system capability should be included.
10. Discussion of reactor core stability. It should include:
- Phenomena and reactor aspects that influence the stability of the nuclear reactor core.
 - Calculations and considerations given to xenon-induced spatial oscillations.
 - Potential stability issues due to other phenomena or conditions.
 - Verification of the analytical methods for comparison with measured data.
11. Description and discussion of analytical methods. It should include:
- Descriptions of the analytical methods used in the nuclear design, including those for predicting criticality, reactivity coefficients, burnup, and stability.
 - The database and/or nuclear data libraries used for neutron cross-section data and other nuclear parameters, including delayed neutron and photoneutron data and other relevant data.
 - Verification and validation of the analytical methods. The discussion of areas for assessment of the validation adequacy should include:
 - a. *Methodology Validation*. Evaluation of the models embedded in the codes along with interfaces, assumptions, correlations, and approximations employed by the full core reactor physics simulation model to ensure that they are capable of simulating behaviour and phenomena relevant to design and safety analysis.
 - b. *Code Validation*. Demonstration that the codes are capable of simulating specific phenomena within some specified tolerance.
 - c. *Phenomena and Key Parameters*. Cross-linking of experimental phenomena and parameters in validation database with design and safety analysis.
 - d. *Domain of Applicability*. Ranges of key parameters in the validation database overlap those expected in design and safety analysis.
 - e. *Accuracy Quantification*. Quantification of the agreement between measurement and code and methodology predictions of key parameters. Accuracy values should have systematic and random (stochastic) components qualified.
 - f. *Scaling*. Scaling of experimental facilities must be sufficiently representative of reactor conditions to support the use of the accuracy calculated from the validation results for key parameters to the reactor calculation.
 - g. *Representation*. May include examination of nuclear data, data transfer between various computer codes, assumptions, approximations, correlations, nodalization, and time-step size.

12. Discussions of the areas concerning irradiation of core internals, such as pressure tubes, calandria tubes, guide tubes, etc. It should include:
- Neutron flux spectrum above 1 MeV in the core, and at the core boundaries.
 - Assumptions used in the calculations.
 - Computer codes used in the analysis.
 - The database for fast neutron cross-sections.
 - The geometric modeling of the reactor core internals.
 - Uncertainties in the calculation.

In the area of fuel limits we note that the current high level requirements for fuel design are not in general complemented by low level limits on safety criteria. These are expected to be developed by the designer and subject to verification and acceptance by the regulator.

The objective of establishing criteria and limits for fuel is to ensure its safe performance in different reactor states, including normal operation and accidents. The underlying principle is that fuel should not fail itself nor should its response lead to conditions which may cause failure of interfacing systems. For more probable transients, the objective is ensure that no or, at most, only very small number of fuel elements would lose integrity; for less likely events the fundamental requirement is to ensure the core coolability.

A large number of experiments were conducted to establish safety criteria and quantify corresponding limits, as well as to advance theoretical understanding of phenomena and develop analytical models. While it is generally considered that there are adequate data and methods to predict fuel response in more likely conditions, there is still the need to continue research for a more adequate fuel design qualification in order to address gaps revealed by new knowledge about core response and transient progression. Extrapolation of existing models outside their database may not be appropriate as has been shown by several threshold effects.

Despite the fact that the overall fuel performance database is extensive, there are some regimes or ranges of conditions for which no or little data are available, for example, because of difficulties in reproducing in-reactor conditions. In such cases the safety limits need to be established conservatively to provide enough confidence that unknown effects would not challenge the safety of fuel performance.

APPENDIX 2

Shutdown System Effectiveness: Regulatory Requirements and Expectations

The regulatory framework for the regulation of CANDU reactor shutdown systems contains a comprehensive set of high-level requirements that establish a firm foundation for high assurance that these systems will perform their safety functions. This framework includes deterministic requirements and unavailability requirements that are akin to risk-informed regulations. The deterministic requirements include the design specifications for two independent and diverse shutdown safety systems and independence of these systems

from the process systems. The unavailability requirements establish performance targets for each shutdown system and performance requirements for the process systems.

Reactors licensed for construction after January 1, 1977 [based on the applicability of Regulatory Document R-10] shall have two full capability reactor shutdown systems, each capable of shutting down the reactor during any postulated accident condition. The two systems shall be functionally and physically independent of each other and of the reactor regulating system. For those plant designs incorporating two independent reactor protective shutdown systems, R-10 states that it is accepted that at least one of them will operate as designed when protective shutdown action is required [R-10, Part II, Section 1.2]. This requirement removes the need to consider the failure of both shutdown systems from the scope of the consequence analysis (siting guide, AECB-1010).

Regulatory Document R-8, "Requirements for Shutdown Systems for CANDU Nuclear Power Plants," [AECB 1991] establishes the specific design requirements for two independent and diverse shutdown systems. It requires each system to be designed such that:

- a) the reactor is rendered subcritical and is maintained subcritical
- b) the reference dose limits are not exceeded and
- c) a loss of primary heat transport system integrity shall not result from any fuel failure mechanism

There is conservative guidance within Regulatory Documents R-10 and R-8 requiring two diverse shutdown parameters for each shutdown system and that for each trip each shutdown system meets the effectiveness requirements. This requirement removes the reliability benefit of the diverse parameter requirements by requiring each parameter to meet the 10^{-3} years per year unavailability requirement. However, this is not satisfied for slow loss of reactivity control scenarios, for example, where only one trip parameter has in general been demonstrated to be effective. In this case failures associated with process instrumentation are significant contributors to the calculated unavailability. Other failures, such as failures of support systems, common cause, external events, and software errors would become potentially significant contributors.

Specific regulatory requirements for trip parameters and their effectiveness are:

- a) R-10 Section 3.5 states that "Where practicable, two diverse trip parameters shall be incorporated into the sensing and control logic of each protective shutdown system for each of the serious process failures requiring shutdown action."
- b) R-8 Section 3.6.1 requires two diverse trip parameters, on each shutdown system, that are capable of meeting effectiveness requirements. Exceptions are allowed for the second trip parameter if it is not practicable or if it is detrimental to safety.

c) The trip parameter acceptance criteria given in G-144 are:

- the primary trip parameter should be capable of preventing the onset of intermittent fuel sheath dryout, and
- the second trip parameter on each shutdown system should prevent sheath temperature from exceeding 600°C, and should prevent the duration in post-dryout from exceeding 60 seconds

The regulatory expectations have been that:

- Margin for lack-of-knowledge uncertainties is built into the selected success criteria (safety limits/derived acceptance criteria). The intent is to allow margin for phenomena and processes that are inadequately considered in generating models to simulate the behavior of a given system or physical barrier. The safety limit is expected to be set below the onset of damage, by an amount that is commensurate with the lack of data. This gives the requisite confidence that the probability of failure will be negligible and some additional margin will be available for unknown events and phenomena.
- The shutdown systems are effective irrespective of probability of the OP&P permitted operating states and initial conditions at the time of postulated event with an adequate margin;
- The cumulative likelihood of severe damage in case of AOOs and DBAs is less than the likelihood of shutdown systems failure on demand. This is to ensure that conditions set in R-10 for not requiring demonstration of adequacy of mitigation provision for anticipated reactivity transients without shutdown are met.

Industry Standards and Practices

The industry current design requirements and practices are governed by the CSA standard CAN3-N290.1-80, "Requirements for the Shutdown Systems of CANDU Nuclear Power Plants," [CSA 1980]. This standard is focused on ensuring that the Shutdown System operates as intended when required and minimizing Shutdown System operation when no potentially hazardous situation exists.

This document was issued in December 1980 and is referenced by Regulatory Document R-8 which states that any aspects of the design which fails to comply with the application requirements contained in this standard shall be identified. The standard provides additional supporting requirements primarily focused on shutdown system design requirements.

The most recent specific design requirements ensuring that the requirements in CSA standard are met were set for Darlington NGS and are (Darlington NGS, Safety Report, Chapter 2, Section 5.2 "Shutdown Systems", paragraph 5.2.1 "Requirements"):

“5.2.1 (2) Following postulated accidents, the shutdown systems should act as necessary to prevent accident release limits from being exceeded. As one means of meeting this criterion for some of the more serious postulated accidents, it has been decided to apply the following requirements:

(a) Each shutdown system shall have sufficient capability considering trip parameters, trip setpoints, signal delay and reactivity insertion rate and depth, such as to prevent pressure tube failure as a result of high energy fuel breakup during postulated loss of coolant accidents.

(b) Each shutdown system shall have sufficient capability, considering trip parameters, trip setpoints, signal delay and reactivity insertion rate and depth, such that a loss of bulk power regulation or a loss of spatial power regulation does not result in pressure tube failure”.

A key requirement in the standard CAN3-N290.1-80 (Requirements for the Shutdown Systems of CANDU Nuclear Power Plants) is to address the analytical failure mode. The analytical failure mode is essentially related to epistemic uncertainties.