(SSL - ONSR - 03)
Rev. 0, 87/09/29

REVIEW OF

ONTARIO HYDRO PICKERING 'A' and BRUCE 'A'

NUCLEAR GENERATING STATIONS' ACCIDENT ANALYSES

Report prepared for

ONTARIO NUCLEAR SAFETY REVIEW

by

K.J. Serdula, Ph.D., P.Eng., FEIC

SERDULA SYSTEMS LIMITED

September, 1987

Serdula Systems Limited

SYSTEMS ENGINEERING CONSULTANTS

REVIEW OF ONTARIO HYDRO PICKERING 'A' and BRUCE 'A' NUCLEAR GENERATING STATIONS' ACCIDENT ANALYSES

Abstract

The Chernobyl accident motivated establishement of reviews of nuclear safety especially in countries with existing nuclear power programs. The work reported here was done under contract to the Ontario Nuclear Safety Review which was established to review the safety of Ontario Hydro's nuclear generating stations. Constraints on resources and time permitted only a limited review of accident analyses available for the Pickering 'A' and Bruce 'A' nuclear generating stations. The reviewed documentation consisted only of results of deterministic safety analyses. Probabilistic based safety analyses were not reviewed.

The methodology used in the evaluation and assessment was based on the concept of "N" critical parameters defining an N-dimensional safety parameter space. The reviewed accident analyses were evaluated and assessed based on their demonstrated safety coverage for credible values and trajectories of the critical parameters within this N-dimensional safety parameter space. The reported assessment did not consider probability of occurrence of event.

The reviewed analyses were extensive, in both breadth and in depth, for potential occurrence of accidents under normal steady-state operating conditions. These analyses demonstrated an adequate assurance of safety for the analyzed conditions. However, even for these reactor conditions, items have been identified for consideration of review and/or further study, which would provide a greater assurrance of safety in the event of an accident. Accident analyses based on a plant in a normal transient operating state or in an off-normal condition but within the allowable operating envelope are not as extensive. Improvements in demonstrations and/or justifications of safety upon potential occurrence of accidents would provide further assurrance of adequacy of safety under these transient and off-normal conditions. Occurrence of some events under these latter conditions have not been analyzed extensively because of their judged low probability of occurrence; however, the accident analyses in this area should be considered for review and/or further study by Ontario Hydro.

Recommendations are presented relating to items discussed above. Additional recommendations are presented for consideration to provide a greater assurrance of the adequacy of the safety provided by the Pickering GS 'A' special safety systems.

TABLE OF CONTENTS

REVIEW OF
ONTARIO HYDRO PICKERING 'A' and BRUCE 'A'
NUCLEAR GENERATING STATIONS' ACCIDENT ANALYSES

1.0 INTRODUCTION

Serdula Systems Ltd. has been contracted by the Ontario Nuclear Safety Review, ONSR, to assist in the execution of its mandate. The specific task undertaken for ONSR was to evaluate and assess the accident analyses done for the Ontario Hydro Pickering 'A' and Bruce 'A' nuclear generating stations by identification of key safety parameters. The scope of this task was delineated by the resources and time made available to the Contractor by the Ontario Nuclear Safety Review. This has resulted principally in a review by the Contractor of the supplied documentation (1,2,3).

This report presents:

- methodology used in the evaluation of the accident analyses,
- evaluation and assessment of the accident analyses,
- conclusions and recommendations.

2.0 REVIEW METHODOLOGY

2.1 Introduction

Licensing of CANDUs for operation in Canada is based on safety analyses which show that in the event of accidents, releases of radioactivity to the public will not exceed prescribed limits. Recent analyses employ two approaches in evaluation of plant safety to provide assurance that requirements are met. These analytical approaches are based on:

- deterministic techniques,
- probabilistic techniques.

Deterministic analyses should show that prescribed radioactive release limits are not exceeded following selected reference (design-basis) accidents. Selected reference accidents to be analyzed must cover not only potential "single failures" but also postulated "dual failures". These latter failures evaluate consequences of single failure combined with failure of a special safety system.(+)

Events selected for deterministic analysis are based on loss of critical safety functions, for example:

- loss of reactor power control,
- loss of coolant inventory
- loss of coolant flow,
- loss of heat sink.

(+) Special Safety systems are provided to maintain critical safety functions upon failure of major process systems to maintain their function within pre-defined limits.

Credible accidents are then selected which characterize "worst-case scenario" losses of the critical safety functions and form the "design- basis" accident sets selected for analysis. For example, typical events selected for analysis to characterize loss of the critical safety functions mentioned above are:

- loss of reactor power control - loss of reactivity control, LORC, events,
- loss of coolant inventory - loss of coolant accidents, LOCAs,
- loss of coolant flow - loss of Class IV events,
- loss of heat sink - feedwater and steam side failures.

Probabilistic analyses are based on generation of event sequences showing plant response following an initiating event. Frequency of the initiating event is determined from fault-tree analysis. Multiple failure combinations are considered. Event sequences are developed until a stable plant condition is attained, consequences are acceptable or frequency of combined events is less than 10^{-7} events per year.

Evaluation and assessment of safety in both of the above approaches is based on occurrence of selected initiating events and determination of the subsequent plant response. Because of the large number of combinations of events and initial conditions, all combinations are not subjected to exhaustive analysis. Events are selected for detailed analysis based on existing information, past experience, engineering and scientific judgement, use of conservative assumptions in analyses, and scope of coverage, for example, "worst case" scenarios.

Consequences of events can be influenced significantly by the initial values and subsequent trajectories, following an event, of a limited number, N, of parameters critical to the safety of the station. These parameters have physical bounds on their amplitudes and rates of change. One can view these parameters as forming an

N-dimensional space where the parameters can have initial values and vary following an event within this N-dimensional space. To ensure safety for all possible accidents, one should ensure safety requirements are met within this N-dimensional parameter space including on the boundaries. Existing safety methodologies, based on analysis of selected events, results in showing safety requirements are met at points or regions in this N-dimensional space. Inherent in these methodologies is the assumption that by showing safety requirements are met for selected events, one can assume that safety requirements will be met throughout this N-dimensional space for credible parameter states.

The above concept of safety in an N-dimensional parameter space has been applied to the evaluation and assessment of accident analyses reviewed in this report.

2.2 N-Dimensional Safety Parameter Space

Safety functions required to ensure public safety following an accident are:

(i) Shutdown of the reactor,
(ii) Removal of core decay heat,
(iii) Contain any radioactive releases,
(iv) Monitor and control of the above functions.

This report is directed towards only the first three items.

Parameters considered in the N-dimensional Safety Parameter Space in the review are:

- reactor power (both global and local) which determines heat production. Reactor power is determined by core reactivity.
- secondary side pressure which determines primary to secondary heat transfer and normally establishes the reactor coolant

inlet temperature.

- primary side pressure which for uncontrolled high values can influence the integrity of the primary heat transport circuit. An uncontrolled low primary pressure without a corresponding decrease in secondary side pressure can reduce primary to secondary side heat transfer with a potential increase in core voiding.
- primary side temperature which for values corresponding to the saturation pressure indicate the presence of coolant quality (core void).
- primary side inventory which for low core inventories can indicate potential degradation of core heat removal capability.
- primary side flows which for low flows combined with high powers indicates a potentially inadequate heat removal capability.
- steam generator levels which establish a capability of the steam generators to transfer heat from the primary circuit to the secondary circuit.
- containment pressure which if high indicates a potential challenge to the integrity of the containment system.
- radiation levels outside the core which if high and not contained can result in potential exposure of the public above accepted limits.

Review of the Safety Reports focused on evaluation and assessment of the capability of the systems, as presented in the analyses, to maintain essential safety functions following an accident. Specifically for the accident analyses presented, noted items, prior to and following the accident, related to the safety parameters given above were:

- variation in amplitude with time,
- projected limits of parameters' variation,
- assessment of derived parameters' value to provide assurance

that the credited safety functions will be maintained.

In regard to parameter limits, the capability of the process systems and special safety systems, prior to and following the accident, to maintain the parameters at the analysed limits was considered in the review. During operation, these parameter limits are set by special safety systems' actions, or automatic regulation system actions or manual operator actions following detection of an off-normal condition.

3.0 EVALUATION OF THE ACCIDENT ANALYSES

3.1 Station Selection

Stations selected for review of accident analyses were Pickering GS 'A' and Bruce GS 'A'. Being the first and second respectively of Ontario Hydro's commercially designed CANDU stations, these station designs may not incorporate:

- evolutionary trends resulting in increased licensing requirements,
- results of subsequent R&D and computer code developments.

3.2 Accident Analyses Reviewed

For Pickering GS 'A' the Restart Analysis (2) was provided for review. Pickering Units 1 to 4 Safety Report is under revision and the previous Safety Report was not current because of completed and/or pending design changes. Only a draft of Volume 1 (1) giving a general description of the station was available to assist in the evaluation of the Restart Analysis. An evaluation of the potential capability of the station to respond to accidents was also undertaken based on the general description provided in Volume 1 (1).

For Bruce GS 'A', Volumes 1, 2 and 3 of the Safety Report (3) were provided for review. Volume 3 presenting the accident analyses did not include any analyses relating to accidents occurring while boosters were in the core. Consequently analyses of potential accidents occurring during booster operation have not been reviewed.

3.3 Assessment Consideration

It is considered difficult if not impossible to eliminate all risk from any human endeavour; electrical generation by nuclear fission

is no exception. If one accepts the previous statement, then one is confronted with answering, "What is an acceptable risk?" No apparently universally accepted defined level of risk exists for electricity generation by fission. Without a clearly defined acceptable level of risk, a judged acceptable level of risk can be strongly influenced by the subjective bias of the reviewer.

Accepting that it is difficult if not impossible to eliminate all risk in any human endeavour, it can also be stated that improvements can be made in most if not all endeavours to reduce the risk. Any improvements to be realized must result in net benefits when all costs (including economic and social costs off-site) are considered. For example, retrofitting a nuclear power station can result in off-site economic and social costs due to loss of electricity production.

The above discussion has been presented to give the reader some insight into the broad range of factors which must be considered in assessment of risk. Although every attempt has been made to be objective, the following assessment may be biased by the subjectivity of the author.

Assessment of areas to be considered for improvement are based on the above discussion and the author's knowledge of the CANDU nuclear power system. In addition, a limited discussion with Ontario Hydro staff (6) had been held based on comments arising from the initial review of the documentation.

3.4 Scope of Review

The accident analyses reviewed focused principally on loss-of-regulation, LOR, and loss-of-coolant accidents, LOCA, presented in the documentation (2,3). The review was directed towards evaluation of the capability of the systems as presented by the analyses to

maintain essential safety functions following an accident. Evaluation of maintaining safety functions was based primarily on noting the analyzed limits of the important safety parameters and the systems credited to constrain these parameters at the given limits.

Establishment of the Ontario Nuclear Safety Review resulted from the accident at Chernobyl. Implications for the safety of the reviewed reactors arising from the following items of significance to the Chernobyl accident were noted:

- positive reactivity effect of voiding,
- safety of the station upon occurrence of accidents in off-nominal operating conditions.

Items reviewed are presented under the following headings:

- reactor shutdown: initiation of reactor shutdown to provide bulk and spatial overpower protection.
- reactivity: during and following an accident, which provides an adequate shutdown of the reactor.
- core heat removal capability: principally removal of fuel heat by the primary heat transport system during and following a LOCA.
- containment: principally a capability to contain any radioactive releases arising from a LOCA.

Significant results of the evaluation and assessment are presented under each of the above items. Generally comments common to both stations are presented followed by specific comments relating to Pickering GS 'A' and Bruce GS 'A', as applicable.

4.0 RESULTS AND DISCUSSION

4.1 Reactor Shutdown

Shutdown of the reactor must be initiated, when the core thermal power production exceeds the existing core heat removal capability, to avoid potential melting of the fuel and subsequent release of radioactivity. This section evaluates and assesses initiation of reactor shutdown on detection of thermal power exceeding heat removal capability. Results are presented in two sections:

- bulk overpower protection,
- spatial overpower protection.

4.1.1 Bulk Overpower Protection

The design of the Ontario Hydro CANDU reactors incorporates many features which reduce the probability of failure to initiate a reactor trip when required. Major features are:

- provision of three independent and identical trip channels for each shutdown system,
- initiation of a reactor trip signal when 2 out-of-3 trip parameters exceed limits,
- independence and diversity of indivdual trip parameters,
- provision of both a principal and a back-up trip parameter, where practical, for the design-basis accident events,
- fail-safe design features for trip parameters,
- annunciation of trip parameter failures,
- on-power periodic testing of trip parameters,
- independence of shutdown systems from the regulation system,
- provision of diversity, independence and physical separation between the trip parameter instrumentations for the two shutdown systems, where provided.

The above design features combine to provide a high availability of shutdown system actuation when required.

Assessment of requirement of shutdown system actions and effectiveness of trip parameters in initiation of a SDS trip signal are based on analyses of trip parameters' responses upon occurrence of selected design-basis accidents over the range of operating conditions. Conservative assumptions are used in the analysis which assesses effectiveness of the individual trip parameters. Examples of conservative assumptions used in the analyses are:

- use of target safety criteria in assessing trip parameter effectiveness which in general are more stringent than the safety design criteria.
- requiring 3 out-of-3 logic to trip which accounts for potential unavailability of a channel.
- not crediting regulation functions to reduce automatically reactor power when important regulated parameters deviate outside pre-selected limits. Crediting this power reduction could eliminate the need for a reactor trip.
- use of trip setpoints which are less conservative than the actual plant trip setpoints to allow for instrument errors and potentially other uncertainties.
- use of conservative assumptions in characterizing fuel bundle powers, channel powers and thermal hydraulic conditions used in the analysis.

Assumptions such as the above provide further assurance that a reactor trip signal will be initiated when required.

The above general features and conservative analysis assumptions provide a general background to the approach used to assure adequacy of initiation of reactor shutdown.

Items of note arising from the evaluation and assessment relating to initiation of a rector shutdown follow.

1. Core power production is not determined directly from measurements by the Pickering GS 'A' and Bruce GS 'A' safety system instrumentation. A single direct measurement giving thermal power production is not possible and a value based on measurements from thermal parameters results in a slow response signal. Changes in neutron/gamma flux, leading changes in thermal power, provide an early signal of thermal power changes. Thus changes in power production are determined from changes in: (a) ion chamber signals measuring neutron flux outside the core and (b) in-core detector signals measuring a combined neutron/gamma flux in the neighbourhood of the detector. These neutronic signals are calibrated manually to the core thermal power production and are subsequently verified periodically and re-calibrated, if necessary. The reference thermal power used in the calibration is based on a value derived from the regulation system instrumentation. This calibration process, providing a link between the safety and regulation systems, provides some loss of the stated independence between safety and regulation systems, between the shutdown systems and among the channels of a shutdown system. The link between and among these systems, being broken by the required manual calibration by the operator, is considered to provide an adequate level of protection between a common-mode failure of thermal power measurement. Furthermore there is redundancy in the thermal power value computed by the regulation system. This value is also backed up by other supporting measurements.

In addition to use of neutronic signals from ion chambers, Pickering GS 'A' has temperature detectors located in the inlets to the steam generators. This thermocouple signal is slow relative to the neutronic signals and provides effective protection for a limited class of events when process parameters are at nominal conditions.

Inherent in the use of the neutronic signals to provide a measure of the thermal power is the assumption that the ratio of the flux at the detector site/thermal power is constant. This ratio can be affected by changes in lattice properties and parameters and reactivity control device configuration. Changes in this ratio at Pickering GS 'A' ion chambers are provided for by the N-16 compensator which provides an on-line calibration of the out-of-core ion chamber signals, including the effect of boron poison in the moderator which affects neutron flux reaching the ion chamber signal. In-core detectors in Pickering GS 'A' provide a linear rate trip signal and are calibrated to thermal power manually. In-core detectors provide both bulk and spatial overpower protection in Bruce GS 'A'. Changes in the ratio (detector flux/thermal power) during normal operation are provided for by periodic monitoring and manual re-calibration if required of the detector signals. These in-core detectors are located in the moderator and therefore will be susceptible to changes in ratio of (moderator flux/fuel flux (power)) with changes in cell properties and parameters which may occur during an accident, for example: voiding of coolant, change in moderator density, etc. Although these effects can be expected to be small, they have not been mentioned. The significance of these effects during accident conditions should be considered for verification.

Both neutronic and process trip parameters are credited to provide regions of effective trip parameter coverage for loss-of-reactivity control, LORC, events. Safety design target effectiveness of trip parameters is assessed with respect to prevention of the onset of fuel centreline melting and excessive heat transport system overpressure. These requirements assure that the principal safety objective, to maintain heat transport system integrity, is met.

A more conservative criterion, prevention of dryout, is used to

establish effectiveness of neutron overpower, NOP, trip setpoints. A range of input data and assumptions is applied in the analysis of LORC incidents. The intention of this approach is that by using conservative assumptions and a spectrum of initial conditions and reactor control device states in the analysis, demonstration of effective trip parameter coverage for these conditions will provide the assurance that coverage is adequate for the complete spectrum of conceivable accident conditions. Actual effectiveness of the NOP trip parameter is based on meeting the safety design criterion upon introduction of different reactivity and/or bulk neutron power transients which span a range exceeding the conceivable transients. Assessment of this approach to establishing NOP trip parameter effectiveness is discussed in the following section 4.1.2 Spatial Overpower Protection.

2. Consistency between assumptions and conservatisms used in LORC analyses for Pickering GS 'A' to that for Bruce GS 'A' has not been investigated in detail. However, it was noted that while conservative assumptions have been used in assessing trip parameter effectiveness for meeting the overpressure safety design target for Bruce GS 'A', a less conservative assumption was used for Pickering GS 'A'. In Pickering GS 'A' both process and neutronic trip parameters are assessed based on crediting 50% of the heat transport relief capacity. For Bruce GS 'A', overpressure protection provided by the trip parameters for LORC events is analyzed both with and without primary heat transport liquid relief credited.

Differing degrees of conservatism used in the accident analyses of different reactors for the same event, can raise potential queries relating to the least conservative analysis. A common set of conservative assumptions, used consistently as far as practical in analyses of all stations for the same event, would eliminate these concerns.

3. Signals from the ion chambers are used directly for trip parameters and indirectly to provide a conditioning signal (*) of the process parameter trips based on neutron power level. A majority of process parameter trips are related to adequacy of core heat removal capability which is not a significant concern for steady-state operation at low power levels. Thus to permit significant process parameter variations occurring normally during reactor startup and shutdown, these process parameter trips are conditioned out automatically at low powers. However, failure of ion chamber signal low when at high power, can result in disabling not only the directly related neutronic trips but also the ion chamber conditioned process parameter trips of the affected channel.

For Pickering GS 'A', failure of the ion chamber low (<2% full power) would result in disabling 7 out of the total 9 trip parameters in a trip channel. This would result in disabling for the affected channel, all credited trip parameters for a small LOCA and all except High Linear rate credited for a large LOCA. Failure would also inhibit initiation of a moderator dump to augment shutdown capability.

For Bruce GS 'A', failure of the ion chamber signal low results in disabling 5 out of 9 trip parameters on an affected SDS1 channel and 4 out of 7 trip parameters on a SDS2 trip channel.

If the "low" failure of the ion chamber signal is not annunciated upon occurrence, it will be detected during the regular trip parameter testing program. Upon detection of the failure, the operator is required to open the channel which would eliminate consequences of the failure. However, since this single failure can result in common-mode failure of trip parameters in a channel which

---

(*) Conditioned process parameter trips are inhibited at a low value of neutron power.

reduces the stated independence of trip parameters, this item should be considered for review for possible improvements.

4. For Bruce GS 'A' two independent and physically separated trip parameter sets are used, one to actuate SDS1 and the other to actuate SDS2. SDS2 trip parameter instrumentation is physically separated from not only SDS1 trip parameter instrumentation, but also from the regulation system instrumentation. For Pickering GS 'A', although independent, the shutdown system instrumentation is not significantly separated physically from the regulation system instrumentation. Also the two independent and diverse shutdown mechanisms in Pickering GS 'A' are actuated by the same set of trip parameter instrumentation. This lack of significant physical separation between shutdown and regulation system instrumentation in Pickering GS 'A' should be reviewed to assure potential common-mode or cross-linked failures will not lead to events with significant adverse safety consequences.

5. In the accident analysis to establish effectiveness of trip parameters, it is generally assumed that prior to the event, the critical parameters are controlled by the regulation system to their nominal values for the existing conditions. The analyses consider inherent errors and uncertainties in the measurement and control of these parameters. Subsequent variations in these parameters arising from the event are considered in the analyses. During normal operation, most of the critical parameters are under the control of the regulation systems. Generally deviations outside a pre-selected band around the nominal operating value result in an annunciation and/or an automatic action to reduce or eliminate potential consequences. Upon occurrence of an alarm, the operator is expected to take action to restore the parameter to its nominal condition. If the operator actions are not immediately successful and no further degradation of the parameter state occurs, the station operation may be continued if within the defined "allowable

operating" envelope. It does not appear that accident analyses included assessment of trip parameter effectiveness for critical safety parameters at limits for all off-nominal conditions within the allowable operating envelope. It is not demonstrated in the reviewed material that conservatisms used in the analyses are sufficient to account for the above conditions. Demonstration of credited trip parameter effectiveness should be considered under conditions of critical safety parameters at limits during off-normal operation. These analyses would consider effectiveness of credited trip parameters when event occurs with trip parameter not at its nominal value but at its alarm setpoint and/or reactor power setback or stepback setpoint.

Some provision for accounting for continued operation during off-normal operating conditions is provided at present by the requirement to change manually trip parameter setpoints upon detection of off-normal conditions. Constraints on continued operation with parameters in off-normal conditions are also defined in station Operating Policies and Procedures and other station operating documentation. This aspect was not reviewed in detail since it is outside the scope of this review.

4.1.2 Spatial Overpower Protection

The spatial distribution of neutron flux and thus thermal power can vary in CANDU reactors dur to changes in the spatial distribution of reactivity devices and local material (e.g., fuel and coolant) properties and parameters. Local overpower must be limited during operation to the existing heat removal capability to prevent fuel melting and a potential consequential release of radioactivity.

1. Spatial overpower protection coverage is provided by the neutron overpower trip parameter and other neutronic and process trip parameters. Assessment of the effectiveness of the NOP trip

parameter for loss-of-reactivity control, LORC, events is based on a selected large set of spatial flux shapes considered to cover the complete spectrum of flux shapes that could result from movement of reactivity control devices during normal operation and under abnormal conditions. These spatial flux shapes are determined from asymptotic static flux calculations for cases where it is assumed spatial control is functioning or is not functioning. Trip setpoints for the flux shapes are determined by a Monte Carlo statistical analysis based on probability of occurrence of dryout when the given flux shape is subjected to a wide range of bulk transients in neutron power. The inherent assumption in this approach is that the spatial distributions of neutron flux and thermal power remains constant during the LORC event with values determined from the flux shape analyzed. The actual bulk and spatial reactivity transients and the resulting neutron and thermal power spatial distribution arising from the motion of the considered reactivity devices from their initial to final state are not simulated.

In discussion with Ontario Hydro staff, they stated that NOP trip setpoints are based on requirements for the most limiting flux shape analyzed for the subset of flux shapes used in establishing the trip setpoint. This results in a very conservative setpoint for all flux shapes in the subset except for the limiting flux shape on which the trip setpoints are based. Even for this flux shape the trip setpoints are considered to be conservative.

Feedback reactivity effects as a consequence of the power increase during a LORC are not considered in the analysis. As the power increases, the fuel temperature increases resulting in an increase in coolant temperature and occurrence of voiding in the channel prior to occurrence of dryout. Resulting effects of these reactivity feedback mechanisms on the spatial flux distribution are considered to result in only second-order effects. It was stated by

Ontario Hydro staff that this assumption arises because the power coefficient, a combination of the reactivity feedback effects, is approximately zero at nominal full power conditions. The zero power coefficient quoted is a description of the feedback reactivity effects on the bulk reactivity. Although effects of local variations in the power coefficient "averaged" over the core may be approximately zero, individual local variations may be significant. The assumption of reactivity feedback effects giving rise to at a maximum second-order effects has not been demonstrated by analysis at the full power condition or at other powers. Inherent in the coverage of the demonstrated analysis is the assumption that coverage of the actual physical transients will be provided by the setpoints established for either the flux shapes related to the transient or by the other flux shapes in the analyzed set.

Variations in channel power relative to the reference power distribution used to determine the trip setpoints are accounted for by application of a channel Power Peaking Factor, CPPF, established relative to a nominal reference distribution. The maximum relative channel power peaking factor, the CPPF, is determined from off-line static flux calculations normalized to the actual core spatial flux distributions and thermal power measurements.

Trip setpoints established for the different flux shapes at power are based on normal heat transport conditions. Effectiveness of the credited trip parameters with the heat transport system in off-normal conditions at power is not demonstrated in the reviewed safety analysis except for Bruce GS 'A' which includes analysis for only 3 out of the normally 4 primary heat transport pumps in operation.

For Pickering GS 'A', the NOP trip parameter for an individual channel is based on a signal from one out of three out-of-core ion chambers located at the periphery of the bottom half of the core

near the central vertical plane. Use of a single signal results in the requirement to adjust trip setpoints (from nominal full power operation values), to provide effective coverage for the potential range of flux shapes during normal (but off-nominal) and off-normal reactivity control device states. The required adjustments are to be performed manually by the operator. Consideration should be given to adjustment of NOP trip setpoints automatically during normal operating transients to reduce demands imposed on the operator under these conditions. Although it is recognized as a low probability event, specific concern exists upon occurrence of a LORC event following initiation of a setback in power and in the subsequent approach of the reactor to an asymptotic state because of the resulting Xenon transient.

For Bruce GS 'A', the NOP trip setpoint is based on a collection of signals from in-core detectors distributed throughout the core. Each of the three logic channels of SDS1 contains at least 12 detectors while there are 4 detectors for each channel of SDS2. The significant number of SDS1 NOP detectors allows a single trip setpoint to be used which allows both an adequate operating margin at normal full power operating conditions and coverage for both normal off-nominal and a wide range of off-normal reactivity device configurations. SDS2 NOP trip parameter nominal setpoint coverage, based on a fewer number of detectors, provides coverage for all except a few off-nominal and off-normal reactivity device configurations. Coverage for LORC transients occurring from these configurations is stated to be provided by a manual change in positions of individual handswitches, one provided for each channel, from their "Normal" position to "Off-normal 1" position.

The design basis set for the Bruce GS 'A' NOP system used 64 and 33 flux shapes for SDS1 and SDS2 respectively. For "unanalyzed flux shapes" coverage is stated to be provided by handswitch in "Off-normal 1" position which results in a reduction in trip

setpoints from their normal value of 118.5% F.P. to 107.9% F.P. The adequacy of this trip setpoint to provide coverage for "unanalysed flux shapes" is not demonstrated.

In contrast to Pickering GS 'A', redundancy in primary heat transport pumps is not provided in Bruce GS 'A'. Coverage for LORC events occurring during a Bruce GS 'A' unit operating with only 3 pumps is provided by manual switching(+) of the NOP handswitches to "Off-normal 2" position. Although Bruce GS 'A' also requires manual action to adjust trip setpoints to provide NOP coverage for LORC events, the required number of adjustments is limited to a maximum of 2 compared to the potentially greater number of trip setpoint adjustments required to provide NOP coverage for the corresponding range of LORC events in Pickering GS 'A'.

2. Both bulk and spatial overpower coverage for LORC events at low power with reduced heat removal capability is provided by both neutronic and the conditioned process trip parameters. The low power log N conditioning level of the process parameter provides the trip (>2% F.P. for Pickering GS 'A', >1% F.P. for SDS1 and >5% F.P. for SDS2 of Bruce GS 'A'). The actual effective steady-state conditioning level is dependent on the moderator boron concentration and for cases of high boron concentration could reduce the neutron flux at the ion chamber by a factor of 1.5 thus increasing by 1.5 the thermal power level at which conditioning comes in. For conservatism, trip coverage is assessed for an effective conditioning power level of 10% F.P. This provides a margin for changes of channel power/ion chamber signal arising from changes in moderator boron concentration and spatial flux distribution. Although 10% F.P. used in the assessment provides an adequate

---

(+) A design change is being made to reduce automatically the NOP trip setpoint on SDS2 when neutron power reduces below a specified level.

margin for Pickering and Bruce SDS1, the margin provided for by the >5% F.P. log N conditioning level of Bruce SDS2 should be considered as an item for review.

4.2 Reactivity

Once actuated, the shutdown system has to insert negative reactivity at a rate and depth to reduce consequences to an accpetable level due to any overpower transient produced by the event. The shutdown system capabilities to meet this requirement are assessed based on the core reactivity transient produced by the event.

4.2.1 Shutdown Reactivity

The capability of a shutdown system to shutdown and ensure shutdown of the reactor is determined firstly by the timely initiation of the shutdown system actuation signals which was discussed in the previous section. The second requirement to ensure adequate shutdown depends on the rate and depth of the negative reactivity inserted by the shutdown system. This latter aspect is discussed in the following section.

1. Bruce GS 'A' has two independent and diverse shutdown systems (one, SDS1, consists of shutoff rods and the other, SDS2, injects a liquid poison into the moderator) providing stated approximately equivalent overall coverage for the analyzed accidents. In general, most of the accident analysis is based on the power increase being terminated by SDS1 action. It was stated by Ontario Hydro staff, although not demonstrated in the reviewed Safety report, that SDS2 provides a greater negative rate and depth of reactivity than SDS1. Even when trip timing used in the analysis is based on SDS2 trip setpoints, it is conservatively assumed the overpower transient is terminated by SDS1.

Pickering GS 'A' has only one rapid-acting completely independent shutdown system, shutoff rods, SORs, which is augmented by moderator dump. Following initiation of a SOR drop signal, the decrease in the ion chamber signal with time is compared against a reference neutron power rundown curve. Moderator dump is initiated automatically if the measured decrease in neutron power with time exceeds the reference rundown curve. This moderator dump provides an independent and diverse reactor shutdown mechanism. It has been stated by Ontario Hydro staff that moderator dump alone (assuming complete unavailability of SORs) provides an effective shutdown for all events except large loss-of-coolant accidents, LOCAs.

Pickering GS 'A' units with their shutdown systems are unique among the Ontario Hydro operating reactors. The Pickering GS 'A' shutdown system, although unique among Ontario Hydro reactors, is similar to other reactor designs operating internationally in the western world wherein only one fast-acting shutdown system is provided. Also in these latter designs, the independence between the shutdown and regulation systems does not exist to the extent of that in the Pickering GS 'A' units.

One may conclude that other Ontario Hydro reactors with two fast-acting, completely independent, diverse and physically separated shutdown systems provide a greater assurance of safety than that provided by Pickering GS 'A' shutdown systems. Assurance of safety provided by the Pickering GS 'A' shutdown system is considered to be adequate if analyses based on recent information and using present computer models confirm information on which the initial Pickering GS 'A' assessment of safety was based.

2. In the reviewed Safety Reports, shutoff rod reactivity worth was assessed based on the assumption that the two most effective rods were unavailable. This assumption was applied only to incidents where damage to the shutoff rods was not postulated. Reactivity

worth of the available rods is determined by the spatial distribution of the neutron flux existing during their insertion. Shutoff reactivity worth credited in LORC and small LOCA analyses is based on a reactivity versus time insertion characteristic assuming existence of the nominal neutron flux spatial distribution. It was stated by Ontario Hydro staff that changes in the spatial flux distribution arising from the above events are not expected to be of significance since for these events, timing of trip initiation is the significant parameter not SOR reactivity rate and depth. The adequacy of this statement is not demonstrated in the reviewed analysis. The author considers this statement by Ontario Hydro valid for slow LORC events and small LOCAs in the small LOCA spectrum. Its validity for intermediate and fast LORC events from the analyzed distorted flux shapes and for large LOCAs in the small LOCA spectrum, especially if an initial off-nominal flux shape exists, should be considered as an item for review.

3. For in-core LOCAs, arising from pressure and calandria tube failure or pressure/calandria tube rupture due to gross channel flow blockage, the accident analyses include postulated damage to the shutoff rods. The reactivity worth is calculated for the shutoff rods outside the potential damage zone assuming that one of these remaining rods is also unavailable. Although not specifically stated, it appears that the calculation of the reactivity worth of the remaining shutoff rods does not consider the possibility that the core could be in one of many distorted flux distributions prior to the time of the in-core LOCA. Although this effect may not be significant in the short term it could be significant in the long term and should be considered for review.

4. For the accident analyses, negative reactivity inserted by the regulation system is not credited to establish effectiveness of reactor shutdown. Calculation of shutdown system reactivity worth does not consider distortions in the spatial flux distribution due

to regulation system action during the event. Furthermore these spatial distortions may affect timing of credited neutronic trip parameters resulting in a delay in initiation of a shutdown system trip. One might conclude that any potential reduction in SOR worth arising from distortions in the spatial flux distribution due to regulation system action will be at least compensated by the negative reactivity introduced by the regulation system. This latter conclusion or the effect of spatial distortions (due to regulation system action) on timing of neutronic trip parameters has not been adequately demonstrated for the analyzed accidents.

4.2.2 Core Reactivity

Control of reactor power is achieved by compensating inherent variations in core reactivity due to changes in reactor conditions through movement of the reactivity control devices. Loss of control of reactor power resulting in overpower can occur when control of the reactivity devices is lost or when an event occurs which results in an increase in core reactivity exceeding the rate and/or depth of the reactivity devices controlled by the regulation system. Upon occurrence of this condition, shutdown system action is required to terminate the overpower transient. The shutdown system effectiveness is assessed based on its capability to overcome the increase in inherent core reactivity due to the event and limit consequences, arising from the overpower transient, to an acceptable level. Variations in core reactivity arise from changes in parameters such as fuel, coolant or moderator temperature, coolant or moderator isotopic purity, coolant density (or void fraction), Xenon and moderator poison.

1. Reactivity feedback effects due to fuel temperature changes and coolant density changes are not considered in the analysis of LORC events. It is assumed that any such contributions would be second-order only since the power reactivity coefficient, which

combines the effects due to fuel temperature and coolant density, is approximately zero at the nominal full power operating condition. It has not been demonstrated that this assumption is valid considering the local reactivity effects of voiding and potential variation of the power reactivity coefficient over the power range from low power to powers at the NOP trip setpoints. Feedback reactivity effects will not be of significance for fast LORCs but could be of significance for slow LORCs where NOP trip coverage is credited.

2. For LOCA events, the occurrence of voiding results in a positive reactivity effect. In contrast to LORCs where the void results from the reactivity transient, during a LOCA, the voiding itself induces the reactivity transient. For small break LOCAs, the reactor regulating system can compensate for most if not all of the void-induced bulk reactivity transient. Although the reactor regulating system may provide compensation for the bulk void reactivity transient, because of its limited range it may not compensate for the spatially induced transient. It is stated by Ontario Hydro staff that the assumption is conservative in this latter case since the resulting spatial distortion could induce a NOP trip and only the process parameter trips are credited in the assessment of trip parameter effectiveness for these events. Pickering GS 'A' accident analysis (2), which could be more susceptible to spatial effects, does not include assessment of core spatial reactivity changes upon occurrence of a small break LOCA during startup and setback transients and for abnormal flux distributions.

3. For large LOCA events, an iterative approach is used between the computer code SOPHT, which calculates the void transient based on an input reactivity transient calculated by SMOKIN, and the computer code SMOKIN, which calculates the reactivity transient based on an input void transient from SOPHT. The iteration process is continued

until agreement is reached. This coupling of the two computer codes is achieved by using a "weighted" SOPHT void fraction as input to SMOKIN. There is no adequate demonstration in the reviewed analyses that this weighting process is adequate or that potential loss of spatial reactivity detail through the void fraction "weighting" process does not have any significant consequences.

4. Differences exist in the comparison of assumptions used in the analysis of in-core LOCAs for Pickering GS 'A' and Bruce GS 'A'. Specifically differences exist in the moderator and coolant D_2O purity and the amount of moderator poison assumed in the analysis. Because of these differences the origin of all differences in results can not be identified, that is, if due to the differences in assumptions or the physical differences in the reactor. Values used in the analysis should be consistent with the operational values and include a sensitivity analysis with conservative estimates of these parameters. It must be noted that the positive reactivity resulting from moderator poison displacement by the coolant is only of concern for in-core LOCAs where it is postulated that the emergency coolant injection system, ECIS, is unavailable. If ECIS is available, injection of H_2O upon ECIS initiation results in a very large negative reactivity insertion which augments the negative reactivity of the shutdown system to ensure an adequate core shutdown reactivity margin.

4.3 Core Heat Removal Capability

During all phases of reactor operation, a core heat removal capability must exist which is adequate to remove the heat generated in the core. Reactor power must be reduced rapidly upon occurrence at high power of a major degradation of core heat removal capability. The required rapid power reduction is provided by both process and neutronic parameters which initiate actuation of the shutdown systems.

The evaluated and assessed limits of critical parameters governing core heat removal capability focused primarily on credited parameter limits during LOCA events since these events pose potentially the greatest challenge to maintaining an adequate core heat removal capability.

1. The reviewed Bruce GS 'A' accident analysis (3) covers a broad spectrum of LOCA type events. Analyses cover both the single failure (initiating event) and a dual failure, initiating failure combined with impairments of the ECIS or containment systems or loss of HT pumps and for some events complete loss of ECIS and all related functions characterized by analysis based on loss of ECIS conditioning signal.

The Pickering GS 'A' analysis (2) covers a broad spectrum of single failure LOCA type events but only a limited number (relative to that for Bruce GS 'A') of dual failure accidents. It is expected that the dual failure accident analyses will be expanded in the current revision process of the Pickering GS 'A' Safety report. Impairments of Pickering GS 'A' ECIS may have a higher probability than for Bruce GS 'A' because of, for example, the single header injection valves existing at Pickering GS 'A' compared to the parallel header injection valves at Bruce GS 'A'. The reviewed Pickering GS 'A' LOCA accident analyses have not considered the potential for failure of one or more header injection valves and potential consequences resulting from such an event. This event should be considered for review.

2. Nearly all of the reviewed LOCA analyses credit continued primary heat transport pump operation. Pickering GS 'A' has analysis for small break LOCAs with loss of Class IV power which results in shutdown of the main PHT pumps. Bruce GS 'A' LOCA analyses include the above analyses and also consider a 100% pump

suction header break, large LOCA, with PHT pumps tripped. Concern had arisen, under LOCA conditions at Bruce type units, relating to integrity of PHT piping because of resulting forces arising from potentially high vibration of the large PHT pumps due to cavitation. This has resulted in addition of a PHT pump trip on LOCA in the Bruce GS 'B' units. It was stated by Ontario Hydro staff that such a design change is in the process of being implemented on the Bruce GS 'A' units.

Similar concerns relating to Pickering units are not as significant because of smaller PHT pumps used in these units. This is supported by results from tests of Pickering GS 'B' PHT pumps under simulated LOCA conditions (7). These tests were specifically designed to confirm the pump's ability to operate through two-phase conditions and to provide data to be used in assessment of capability of PHT piping to maintain its integrity under these conditions. Measurements of pump flow under two-phase and single-phase steam conditions made during the tests are considered unreliable because the flow transmitter was calibrated for single-phase liquid flow. Observations and results from the tests do not directly support the relatively high mass flows predicted by SOPHT under conditions of high void in the pump suction header. Observations indicate the pump starts running in steam ("vapour-locked") at relatively low values of loop average void fraction. It is recommended the following areas be considered for review:

- reliability of credited beneficial aspects of maintaining PHT pumps in operation during LOCA,
- potentially negative aspects such as delaying and/or impairing ECI because of potentially early entry and delayed exit of single-steam-phase operation of PHT pumps during a LOCA,

- potential of occurrence and consequence of single-steam-phase operation of PHT pumps upon occurrence of an internal LOCA(+) and/or following initiation of a shutdown for this event.

3. Heat removal capability is strongly dependent on maintaining an adequate coolant inventory. There is no trip parameter which responds directly to a low inventory of coolant in the core. THere is a trip parameter based on low pressurizer level for Bruce GS 'A'. The pressurizer connected to the main PHT piping is credited to provide an effective trip for small LOCAs which discharge external to the PHT system. For some internal LOCAs(+), the pressurizer level can rise as inventory is transferred from the core to the pressurizer and other vessels outside the main PHT circuit. For these latter events and other small LOCAs, the heat transport low pressure, heat transport gross low flow, pressurizer low level, manual and neutron overpower trip parameters are credited to provide effective trip parameter coverage. Consequences of loss-of-coolant inventory occurring on a large LOCA are terminated by the neutronic trip parameters actuated by the reactivity transient resulting from the voiding occurring because of the loss of inventory. Areas to be considered for review arising from this latter type of event were discussed in Section 4.2.2.

Pickering GS 'A' does not have any trip parameters measuring directly low coolant inventory in the core. There is, however, a setback in power by the regulation system on occurrence of high bleed condenser level. This high level could occur on certain internal LOCA events. Analyses pertaining to internal LOCA events were not given in the reviewed document (2) but can be expected to be included in the revised Safety Report. The evolution and

---

(+) An internal LOCA results in transfer of D_2O coolant inventory from the main circuit to storage vessels outside the circuit, which upon filling can result in a discharge outside the PHT system.

consequences of these internal LOCA events can be affected significantly by regulation, process control and safety system actions. It is recommended this area be considered for review especially for Pickering GS 'A' which does not have a pressurizer like Bruce GS 'A' but a pumped-feed and bleed system to maintain core inventory and pressure.

4.4 Containment

The containment system provides a barrier to the release of radioactivity to the public. Occurrence of a large LOCA poses a major challenge to the integrity of the containment due to an increase in containment pressure because of the discharge of hot pressurized coolant. Maintaining containment integrity during the event is of major importance because of a potentially significant release of radioactivity inside containment due to fuel failures. Consequences of potential radioactive releases inside containment must be analyzed to demonstrate that an adequate level of safety is provided by the system.

1. In Ontario Hydro units the pressure within containment during normal operation is kept slightly sub-atmospheric. Buildup of pressure within containment during events such as LOCAs is vented automatically to the vacuum building. Buildup of steam pressure within the vacuum building is terminated by automatic initiation of a water spray system which condenses the steam. The self-actuating dousing mechanism is dependent on maintaining adequate water levels in the main water storage tank and in the downcomer water seal which provides isolation of an upper vacuum chamber from the main building volume. Maintenance of adequate water level in the downcomer water seal is essential for self-actuation of the dousing system.

This water level in the downcomer water seal of the Bruce GS 'A' vacuum building is monitored by duplicated level measuring

instrumentation. If levels deviate outside defined limits, an alarm is annunciated in the main control room.

Adequacy of water level in the downcomer water seal of the Pickering GS 'A' vacuum building is assessed by monitoring overflow resulting from continuous makeup to the spray headers. A low flow is annunciated in the main control room indicating a potential loss of water from the downcomer water seals. Low flow can be confirmed from observations of individual "sight glasses" in the header overflow lines.

It is recommended for both stations consideration be given to a review of the need for detection of "as-is" failures of low water-seal level diagnostic transmitters such as could be provided by independent periodic on-line testing of these transmitters. A reliability assessment for Bruce GS 'B' containment system (8) addressed this aspect and predicted an unavailability of 5.9×10^{-3} year/year for dousing. However, fouling of the make-up water line preceded by an "as-is" failure of a level transmitter, a "low probability event", was not addressed.

2. During small to intermediate LOCAs dousing may cease shortly after initial actuation because of the rapid reduction in vacuum building pressure. Subsequently vacuum building pressure may build up again. It is recommended a review be considered of the need for multiple initiation of the dousing system upon occurrence of a LOCA and the potential capability of the dousing system to meet requirements.

3. Consequences of radioactivity releases arising from LOCAs have been analyzed for Pickering GS 'A' and Bruce GS 'A' for conditions of the containment performing as designed and for minor impairments of containment. Radioactivity releases are well within permitted release limits for the analyzed conditions.

4. Bruce GS 'A' accident analyses resulting in a "worst-case" containment pressure build-up scenario give a containment pressure approaching the containment test pressure. It was stated by Ontario Hydro staff that containment integrity will not be impaired under these conditions because of the short duration of the high pressure (less than 10 seconds) and the approximately 60 second overpressure period. Ontario Hydro staff also stated that consequences of a large LOCA with coincident loss of dousing were analyzed for Bruce GS 'B'. However, a review of these results as to their applicability to Bruce GS 'A' was not made.

5. The Bruce GS 'A' steam pressure is vented into the vacuum building by discharging through vertical ducts. Upon initiation of dousing, water could potentially enter these ducts. It is recommended consideration be given to a review of the range of potential consequences that could arise upon entry of water into these discharge ducts.

4.5 Summary of Assessment

The scope of the reviewed accident analyses embodies considerable breadth and depth especially for Bruce GS 'A'. This review did not include accident analyses pertaining to operation with booster fuel assemblies for Bruce GS 'A' since such analyses have not been incorporated into the Bruce GS 'A' Safety Report. Such analyses have been submitted to the AECB, which has permitted the present booster mode of operation at Bruce GS 'A'. A qualitative assessment of accident analyses is presented based on potential occurrence of accidents during the following plant conditions:

- normal steady-state power operating conditions,
- transients arising from normal operating conditions such as power changes, startup and shutdown,

- off-normal operating conditions where one or more critical safety parameters is stabilized at off its normal value but within the defined operating envelope.

The following comments are based only on the reviewed material since all material prepared by Ontario Hydro to support safety and licensing of operation was not reviewed. Detailed review of all such material in the available time was not possible.

Extensive analyses have been undertaken by Ontario Hydro of potential accidents, and their consequences, occurring with a unit at a steady-state power level. This is the condition at which the plant is considered to spend most of its operating life. It is considered, subject to the items noted in the previous sections, that the presented accident analysis for the plant in this condition provides an acceptable assurance that adequate public safety does exist. This statement is predicated on occurrence of the analyzed accidents and their subsequent evolution within the analyzed limits. With implementation of the recommendations, it is considered that the extensive coverage of the analyzed accidents at the steady-state power conditions also provides assurance of public safety for unanalyzed accidents from the nominal full power state.

Reviewed analyses for occurrence of accidents during the transient operating conditions are not as extensive as for the steady-state conditions. Occurrence of LORC accidents under normal operating transient conditions is fairly complete but consequences of occurrence of other accidents such as LOCAs under the transient conditions is not demonstrated for all conditions. It was mentioned by Ontario Hydro staff that for these events, where an adequate level of safety is not adequately demonstrated in the Safety Reports, assurance of adequate safety for potential occurrence of accidents under normal transient conditions is provided by the demonstrated safety following potential occurrence of the same

accidents under normal steady-state operation. Justification of Ontario Hydro's extension of the consequences of steady-state analyses to the transient conditions was based primarily on use in the analyses of "worst-case" accident scenarious and conservative assumptions. Transient cases selected by Ontario Hydro for analysis were based on scientific and engineering judgement and probability of occurrence of events.

It is recommended a review be considered to justify or demonstrate, where not demonstrated, accident analysis coverage or lack of it for occurrence of accidents for the full range of normal transient operating conditions.

Except for limited coverage of accidents occurring during three or two pump operation for Bruce GS 'A', limited discussion or demonstration of accident analyses coverage existed for the reviewed analyses for occurrence of accidents with parameters in an off-normal condition but within the defined operating envelope. The probability of this dual failure event (occurrence of off-normal condition combined with probability of occurrence of accident) is considered low. However the actual probability will be strongly dependent on time to restore system to nominal conditions which is dependent on actions by the station operator, an area outside the scope of this report. It is recommended consideration be given to a review of: the accident analysis, the station operating documentation and/or computed probability of occurrence of events, to ensure that an adequate level of safety does exist upon potential occurrence of accidents under the allowable off-normal operating conditions.

The above areas, recommended to be considered for review, may have been considered in other Ontario Hydro documents which have not been reviewed by the author.

4.6 Impact of Ontario Hydro Work In-Progress

Ontario Hydro has work in progress, related to the scope of the report, to:

- revise and update the Pickering GS 'A' Safety Report,
- incorporate in the Bruce GS 'A' Safety Report existing documentation which demonstrates acceptable consequences from potential occurrence of accidents during presently allowed operating modes with booster fuel assemblies in the core.

It is expected that the completed above work will address some of the recommendations expressed in this report.

Following the accident at Chernobyl, the AECB undertook an evaluation of the implications of this accident on the safety of CANDU reactors (9). Nine areas for studies or review have been recommended in the report. Ontario Hydro has addressed or made a commitment to address in the near future, these recommendations. The first three recommendations, items 1, 2 and 3 listed below, directly applicable to this study, are:

1. The safety analyses of CANDU reactors should be re-examined by the reactor designers and operators to confirm that shutdown systems are sufficiently effective under all possible conditions. Particular attention should be given to events in which a rapid increase in the volume of steam in the fuel channels may occur, or in which there may be rapid increase in reactivity.

2. Various configurations of reactivity devices in CANDU reactors should be examined by the reactor designers and operators to ensure that it is not possible to put the reactor into a condition in which the shutdown systems might be rendered less than adequately effective. This should include an examination of the capability of the shutdown systems under conditions in which there are spatial

variations in reactivity.

3. The safety of the Pickering GS 'A' reactors should be re-examined by Ontario Hydro and the AECB, particularly with respect to accidents involving failure of the reactor control system and loss-of-coolant accompanied by unavailability of the shutdown system.

Another item, item 5, although not directly in the scope of this study, has influence on required depth and breadth of demonstration and/or justification of adequacy of the presented accident analyses to ensure an acceptable level of safety exists upon occurrence of accidents with station parameters off-nominal but within the defined allowable operating envelope or range of values.

This item 5 of the AECB recommendations is:

5. The AECB and plant owners should review, and if necessary increase, the frequency and extent of monitoring and auditing the performance of plant operators in complying with operating procedures, the Operating Policies and Principles and the conditions of Operating Licences.

An item identified in this study, but beyond the scope of this report was that the station operating documentation should be considered for review to ensure operating conditions are constrained to those whose consequences upon potential occurrence of an accident have been justified or demonstrated by accident or other analyses to be acceptable.

It is expected that Ontario Hydro's studies carried out in response to the above recommendations in the AECB report will address also most of the recommendations in this report.

5.0 CONCLUSIONS

An evaulation and assessment of Ontario Hydro Pickering GS 'A' and Bruce GS 'A' deterministic accident analysis has been made based primarily on material presented in references (1,2,3). Resource and time constraints did not permit a detailed review of all accident analyses prepared by Ontario Hydro which demonstrate safety of these installations. Extensive analyses, especially for Bruce GS 'A' have been provided for a broad spectrum of potential accidents occurring under normal steady-state operating conditions and provides an adequate assurance that consequences are within acceptable limits for the accidents presented. Within the above comprehensive analysis, items have been identified for consideration of review and possible actions by Ontario Hydro. Addressing these items would provide further assurance that an adequate level of safety exists upon occurrence of an accident.

Analyses addressing consequences of potential occurrences of accidents during normal transient conditions or steady-state operation with one or more major parameters in off-nominal condition but within the allowable operating envelope are not as comprehensive as for normal steady-state conditions. If was stated by Ontario Hydro staff that in addition to the specific accident analyses provided for these operating conditions, demonstrated assurance of adequate safety for potential occurrence of accidents under normal steady-state operation can be extended, because of the conservatism in the analyses assumptions, to these other operating conditions. It was further stated by Ontario Hydro staff that areas where such an extension is not applicable are low probability events and detailed accident analyses were not done. The author recognizes that these are low probability events when one considers fractional operating lifetime spent in these states combined with probability of occurrence of an accident when in one of these states. However, it must be recognized that the probability of occurrence of an

accident during normal transient or off-normal operating conditions can differ from that during steady-state normal operation. This should be considered in assessing the probability of occurrence of the combined event.

It is concluded that improvements could be made in demonstrating or justifying that an adequate level of safety exists for occurrence of accidents when the unit is operating in normal transient conditions or in off-normal conditions which are within the allowable operating envelope.

General recommendations are presented in the following section. It is possible that these recommendations may have been addressed already by Ontario Hydro since all the Ontario Hydro documentation demonstrating adequacy of safety has not been reviewed. Furthermore it is expected that most, if not all, of the recommendations will be addressed by Ontario Hydro in its committed response to the recommendations in the AECB report (9) on implications for the safety of CANDU reactors based on the accident at Chernobyl.

6.0 RECOMMENDATIONS

The major recommendations presented in Section 4.0 of the report are summarized below. These recommendations are presented to provide further assurance that an adequate level of safety exists in the operation of Ontario Hydro's nuclear generating stations, specificially Pickering GS 'A' and Bruce GS 'A'. It is recommended the following items be considered for review or further study and possible actions by Ontario Hydro.

1. Improvements in demonstrated analyses and/or justification of existence of adequate safety upon potential occurrence of accidents when the unit is not operating in normal steady-state conditions with critical parameters at their nominal conditions. Specifically the allowable operating envelope and constraints defined by station operating documentation (an area outside the scope of this study) should be compared against the operating envelope used in the accident and other analyses to assess acceptability of risks permitted by the station operating documentation.

2. More consistency, as far as practical, in application of conservative assumptions to accident analyses demonstrating consequences on potential occurrence of the same class of accidents but at the different Ontario Hydro reactor designs.

3. Additional demonstration and/or justification of methodology used to determine both bulk and spatial reactivity effects, due to voiding during a LOCA, on resulting neutron power transients and potential consequences arising from uncertainties due to the applied methodology.

4. Further justification and/or verification that unanalyzed consequences are not significant which arise from spatial power transients due to local reactivity effects, including reactivity

feedback, during accidents such as small loss-of-coolant accidents, LOCA, and loss-of reactivity control, LORC, events.

5. Need for establishment of lower bound of shutoff rod, SOR, reactivity worth, for accidents which do or do not result in potential inhibition of insertion of some SORs, based on sensitivity analyses of effects on computed SOR reactivity due to potential distorted spatial flux distributions which could exist at time of SOR actuation.

6. Review of consequences arising from common-mode failure or inhibition of trip parameters in a channel due to failure of a shutdown system ion chamber signal, especially a Pickering GS 'A' ion chamber signal failure.

7. Expansion of existing assessment of consequences of continued primary heat transport pump operation during LOCAs to include effects on maintaining core heat removal capability arising from two-phase and single steam phase operation of the pumps.

8. Need for initiation of potential multiple dousing starts during a small to intermediate LOCA and the capability of the existing dousing systems to meet these requirements.

9. Need of an on-line periodic testing capability of parameters critical to operation of the self-actuating dousing mechanism.

10. Items, applicable to the Pickering GS 'A' station, are:

(i) Update of analyses using recent information and models to confirm results on which the initial assessment of adequacy of safety provided by the shutdown system was based.

(ii) Susceptibility and consequences of common-mode and

cross-linked failures among the independent regulation and protection system instrumentation channels.

(iii) Replacement of required manual adjustment of neutron overpower trip setpoints during normal operating transients by automatic switching.

(iv) Improvements in demonstration of adequacy of emergency core injection system, ECIS, to provide core cooling capability with minor impairments such as failure of one or more header isolation valves to open on demand of the ECIS operation.

(v) Requirement of systems to maintain automatically critical safety functions upon occurrence of a "small" LOCA.

11. Other minor items are presented in Section 4.0.

As noted in the conclusions, it is possible the above items have been addressed in other Ontario Hydro documentation not reviewed by the author or will be addressed in Ontario Hydro's response to the recommendations in a recent AECB report (9).

7.0 REFERENCES

1. Pickering Generating Station 'A' Safety Report, Volume 1. (Revised version in draft form.)

2. Pickering NGS 'A'; Units 1 and 2 Restart Analysis, OH Report 85362, October 1985.

3. Bruce Generating Station 'A' Safety Report, Volumes 1&2, Volume 3, Sections 1, 2, 3.1, 3.2, 3.3, 3.3.1.5, 3.4, 3.5, 3.6, 3.7, 3.8(Draft) and 3.9.

4. AECL Submission to the Ontario Nuclear Safety Review, AECL-9427.

5. Ontario Hydro Submission to the Ontario Nuclear Safety Review.

6. Ontario Hydro: private communication (Gianni M. Frescure, Alan L. Wight, Henry Wong, Paul Burchette and Jim Blyth).

7. "Pickering NGS B Assessment of Primary Heat Transport Pump Loss of Coolant Accident Tests", OH Report 83328.

8. "Bruce GS 'B' Containment Reliability Review", Ontario Hydro Design and Development Division Report No. 81262.

9. "The Accident at Chernobyl and Its Implication for the Safety of CANDU Reactors", INFO-0234 (E), Atomic Energy Control Board, May, 1987.