21st Conference of the Canadian Nuclear Society
Toronto, Ontario, Canada / June 11-14, 2000

# BRUCE B RISK ASSESSMENT: RESULTS & APPLICATIONS

R. Parmar, W.A. Webb, V.M. Raina
Ontario Power Generation
700 University Avenue
Toronto, Ontario, Canada, M5G 1X6
(416) 592-4350

Abstract: This paper describes the major results of the recently-completed Bruce B Risk Assessment (BBRA). The results are presented in the form of the frequencies of various fuel damage categories (FDCs) and ex-plant release categories (EPRCs). Some of the dominant sequences leading to these categories are discussed. Also discussed are the key conclusions of the assessment.

The paper also discusses how the products of the study have been used to support decision-making at the plant. Some specific examples are included. The paper concludes by describing the work undertaken to develop an on-line risk model that is being used on a regular basis by plant personnel to assess the risk impact of changes in plant configuration.

## I. INTRODUCTION

The Bruce B Risk Assessment (BBRA) was issued by Ontario Power Generation (OPG) in January 1999. The BBRA is a comprehensive risk assessment of the Bruce Nuclear Generating Station B, a four-860 MW(e)(net) unit station of CANDU pressurized heavy water reactor design. The BBRA was conducted with the following key objectives:

(a) to review the adequacy of the safety of the station design and operation by means of preparing a risk model for the station, and

(b) to prepare a risk model in a form that it can be used to assist the safety-related decision-making process throughout the life of the station.

The major numerical results of the BBRA representing the various aspects of the risk from operation of Bruce NGS B were reviewed against the applicable Ontario Power Generation, Nuclear (OPG,N) risk-based safety goals [1].

## II. OVERVIEW OF BBRA PROCESS

In order to meet the main objective of evaluation of the safety of the station design and operation, the major task of the BBRA was the identification of the various accident sequences that have the potential to cause a significant release of radioactivity outside the reactor containment, and the estimation of the frequencies of their occurrence and the radiological consequences. Typically, each such sequence is the result of an initial malfunction, or initiating event, followed by failures of other functions or systems designed to mitigate its effects. As the number of sequences with the potential to cause a significant release is potentially very large it is not feasible to explicitly estimate the consequences of each of them. The sequences are therefore categorized by the severity of the associated release of radioactivity (a common practice in Probabilistic Risk Assessments (PRAs)).

Two categorization schemes were utilized in BBRA. The first dealt with the accident sequences that would result in the release of radioactivity from the fuel. Such accident sequences were categorized based on the extent of the associated fuel damage, giving rise to various fuel damage categories (FDCs). Next, the response of the containment system to the occurrence of fuel damage categories was assessed, identifying in the process those containment subsystems whose failure, given the occurrence of fuel damage inside containment, would lead to radioactivity release from containment. The various combinations of fuel damage categories and containment failures were categorized, based on magnitude and timing of radioactivity release to the environment, into ex-plant release categories (EPRCs).

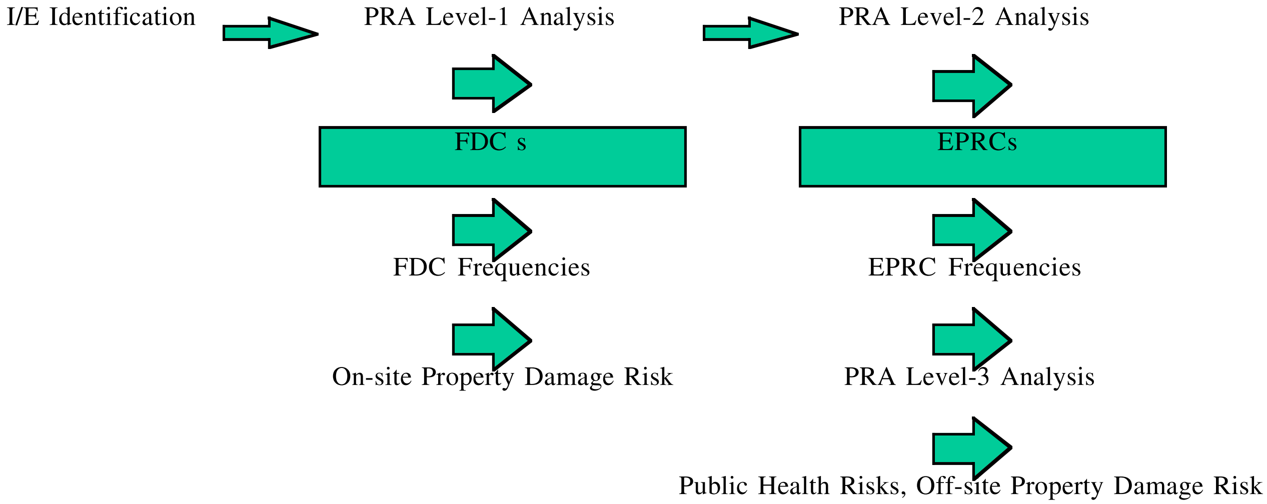


FIGURE 1 BBRA PROCESS

The results were expressed in terms of the expected number of occurrences of each consequence category per unit time. The calculations were performed by following the process of initiating event identification, plant and containment event tree analysis, system fault tree analysis, and the integration of the event and fault tress. Due to the large number of systems modelled, and the significant complexity of many systems, computer-aided methods were used to carry out such computations. For each consequence category, the magnitude of the associated consequence was calculated. This involved environmental release calculations, assessment of damage to public health and property, and determination of financial loss.

In common probabilistic risk assessment parlance, the BBRA is a Level 3 PRA that includes assessments of risk during both at-power and outage states. A Level 3 PRA, by definition, comprises the following [2]:

(a) An analysis of plant design and operation focused on the accident sequences that could lead to fuel damage, their basic causes, and their frequencies (Level 1 PRA).

(b) An analysis of the physical processes of the accident and the response of the containment (constituting, in addition to the analysis performed in a Level 1 PRA, a Level 2 PRA). Besides estimating the frequencies of fuel damage sequences, it predicts the time and the mode of containment failure as well as the inventories of radionuclides released to the environment.

(c) An analysis of the transport of radionuclides through the environment and of the public health and economic consequences of the accident (constituting, in addition to the analysis performed in a Level 2 PRA, a Level 3 PRA).

The overall BBRA process is shown in Figure 1.

TABLE 1
Frequencies of Fuel Damage Categories

| FDC Type | Description | Frequency (occ./year) |
|---|---|---|
| FDC1<br>At power<br>Shutdown (-SD) | Rapid loss of core structural integrity | $6.0 \times 10^{-8}$<br>$6.0 \times 10^{-8}$<br>$8.3 \times 10^{-10}$ |
| FDC2<br>At-power, inside cont. (-IC)<br>At-power, outside cont. (-OC)<br>Shutdown, inside cont. (-SD-IC)<br>Shutdown, outside cont. (-SD-OC) | Slow loss of core structural integrity | $6.4 \times 10^{-5}$<br>$5.2 \times 10^{-5}$<br>$5.2 \times 10^{-6}$<br>$5.9 \times 10^{-6}$<br>$7.2 \times 10^{-7}$ |
| FDC3<br>At-power, inside cont. (-IC)<br>At-power, outside cont. (-OC) | LOCA and early failure of ECI | $9.5 \times 10^{-5}$<br>$8.2 \times 10^{-5}$<br>$1.3 \times 10^{-5}$ |
| FDC4<br>At-power, inside cont. (-IC)<br>At-power, outside cont. (-OC) | LOCA and late failure of ECI. Loss of heat sink. | $9.3 \times 10^{-5}$<br>$6.2 \times 10^{-5}$<br>$3.1 \times 10^{-5}$ |
| FDC5<br>At-power, inside cont. (-IC)<br>At-power, outside cont. (-OC)<br>Shutdown, inside cont. (-SD -IC)<br>Shutdown, outside cont. (-SD -OC) | Small LOCA and late failure of ECI | $1.5 \times 10^{-4}$<br>$4.7 \times 10^{-5}$<br>$6.2 \times 10^{-5}$<br>$3.9 \times 10^{-5}$<br>$3.8 \times 10^{-6}$ |
| FDC6 | Temporary loss of cooling to fuel in many channels | $1.0 \times 10^{-4}$ |
| FDC7 | Single fuel channel failure with sufficient release of steam to initiate automatic containment button-up on high pressure | $3.5 \times 10^{-4}$ |
| FDC8<br>At-power, inside cont. (-IC)<br>At-power, outside cont. (-OC) | Single fuel channel failure with insufficient release of steam to initiate automatic containment button-up on high pressure | $4.7 \times 10^{-3}$<br>$3.3 \times 10^{-3}$<br>$1.4 \times 10^{-3}$ |
| FDC9 | LOCAs which, due to ECI initiation, do not result in fuel overheating but have the potential for significant economic impact | $2.5 \times 10^{-2}$ |

## III. FUEL DAMAGE CATEGORIES

The BBRA study identified a wide variety of fuel damage categories ranging from rapid core structural integrity, FDC1, to single fuel channel failure, FDC8 (see Table 1). A unique feature of the Bruce NGS B containment envelope is that maintenance work can be conducted on a number of major components from outside the containment structure, such as the heat transport (HT) main pumps, the reactivity mechanisms, and the HT feed pumps. It does, however, open up the possibility of containment being bypassed in some fuel damage accidents. To recognize this potential and assess its significance, additional fuel damage categories were defined, with the same labels as above except with the suffix -OC (for outside containment).

The BBRA Study also assessed the causes and likelihoods of fuel damage when the reactor is in a planned outage. Thus, additional fuel damage categories were defined, with the designator -SD used in their labels. The categories FDC1, FDC2, and FDC5 adequately covered the types of fuel damage events that can be expected during the shutdown state.

A description of categories, FDC1 and FDC2, and their key contributors is provided below in detail, while other FDCs are described briefly. FDC1 and FDC2 are selected because both lead to severe core damage.

## A. FDC1

Fuel damage category FDC1 represents sequences involving a rapid loss of core structural integrity (~ seconds) and results if the reactor fails to be shut down when required. As Table 1 shows, the likelihood of such an event is very low. The existence of two shutdown systems, shutdown system 1 (SDS1) and shutdown system 2 (SDS2), with at least two effective trip parameters on both systems for most transients, together with the ability of the reactor regulating system's power reduction features, viz., the Setback and Stepback functions, leads to very low predicted failure frequencies.

The events that dominate are those for which there is either a common failure mode between the two shutdown systems, or only one automatic trip parameter. For example, during very low power operation, only the low power neutron overpower (LNOP) trip can be credited in the event of a slow loss of regulation (LOR) of reactor power. Operator action is required in the main control room to establish SDS trips before the low power state is entered. Failure of the operator to carry out this action leads to impairment of both SDS1 and SDS2 during this operating mode. Likewise, loss of moderator cooling or flow is protected by a setback and SDS1 trip on moderator high temperature, there being no automatic trip on this parameter on SDS2.

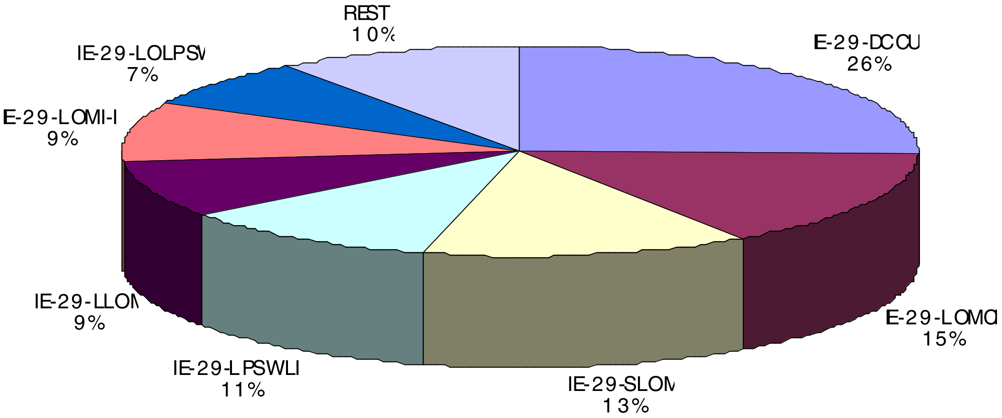


FIGURE 2
IE Contribution to FDC1 (At-power)
Mean Frequency: 6.0 x $10^{-8}$ occ/reactor-yr

Dominant initiating event contributors to FDC1 are shown pictorially in Figure 2. Unsafe dual computer failure and losses of moderator cooling or flow are found to be the most significant. Among the causes of the latter event are losses of low pressure service water initiating events.

## B. FDC2

Fuel damage category FDC2 represents a total loss of core cooling leading to fuel channel failures and, ultimately, calandria vessel failure. FDC2 sequences differ from those in FDC1 primarily in the time at which core damage occurs, usually requiring several hours or more before heat removal is completely lost.

Contributors to this event invariably comprise a loss of coolant followed by failure of all means of coolant makeup, with the additional failure of the moderator to remove decay heat through pressure tube and calandria tube contact. Events in FDC2 lead to a large quantity of fission products being released into the containment building. The frequency of FDC2 from all analyzed contributors is 6.4 x $10^{-5}$ per reactor-year. Given this frequency and the extent of associated fission product release into containment, FDC2 is by far the most important of all fuel damage categories from the perspective of controlling risk.

A dominant accident sequence in FDC2 arises from an intermediate-size powerhouse steam line break with discharge between 100 kg/s and 1000 kg/s followed by failure of the powerhouse venting panels to open. For breaks in this range, the discharge rate is not high enough to either result in automatic opening of the powerhouse vents or a prompt automatic reactor shutdown induced by the resulting low HT system pressure or low boiler level. As a result, steam and hot water discharge into the powerhouse, leading to failure of unqualified equipment located in the powerhouse, such as the Class I/II/III/IV power systems, the unit and common instrument air systems, and the service water systems, constituting the Group 1 set of systems. Although the operator is considered to be highly likely to open the powerhouse vents, hardware failures such as failure of the single initiation pushbutton and associated logic can occur thereby resulting in the failure of Group 2 systems such as emergency power system and the emergency water system. Failure of the unit's Group 1 and Group 2 services leads to failure of the steam generator, shutdown cooling, maintenance cooling and moderator heat sinks as well as of the emergency cooling injection (ECI) system. A few pressure tubes fail and a loss of coolant accident (LOCA) occurs via the annulus gas bellows and possibly a fuel channel.

Lack of automatic initiation of the powerhouse emergency venting system following intermediate secondary side breaks has been recognized, and design modifications are underway to improve the reliability of this system by removing the dependence on operator action.

Even if the powerhouse emergency venting system operates successfully following a secondary system pipe break, the loss of Group 1 systems can by itself initiate a loss of HT coolant. For example, loss of unit instrument air can lead to the opening of HT system liquid relief valves. The bleed condenser will subsequently fill and, unless the operator takes action to reduce the HT pressure, the bleed condenser relief valves could lift. Failure of one or both of the bleed condenser relief valves to reclose leads to a LOCA thus resulting in severe core damage.

The bleed condenser relief valves have recently been replaced on all units with valves of an improved design. The likelihood of these valves failing to close should, therefore, be less than assumed in the BBRA Study, thus reducing the safety impact of the above core damage sequence.

Other significant accident sequences are the ones initiated by condenser cooling water line breaks and low pressure service water (LPSW) failure. An unmitigated condenser cooling water line break can cause partial loss of the Class III system due to flooding thus leading to impairment of the service water and instrument air systems. The subsequent failure of the bleed condenser relief valves is then sufficient to cause severe core damage. LPSW failure can lead to total failure of both HT pump seals thereby resulting in a loss of coolant outside containment.

The key initiating event contributions to FDC2 events inside containment, which form the major component of severe core damage events, are shown in Figure 3. High energy pipe break initiating events are seen to be the most important, with about two-thirds of the frequency of this category being attributable to intermediate steam line breaks.

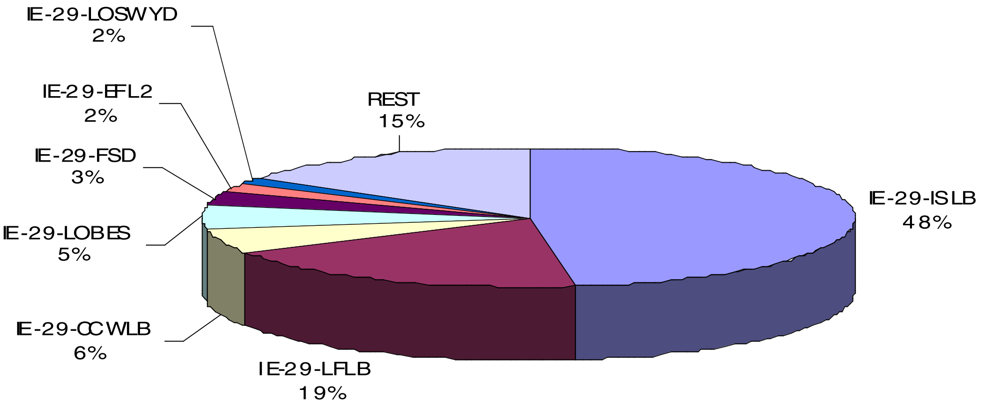


FIGURE 3
IE Contribution to FDC2-IC (At-power)
Mean Frequency: 5.2 x $10^{-5}$ occ/reactor-yr

## C. SEVERE CORE DAMAGE

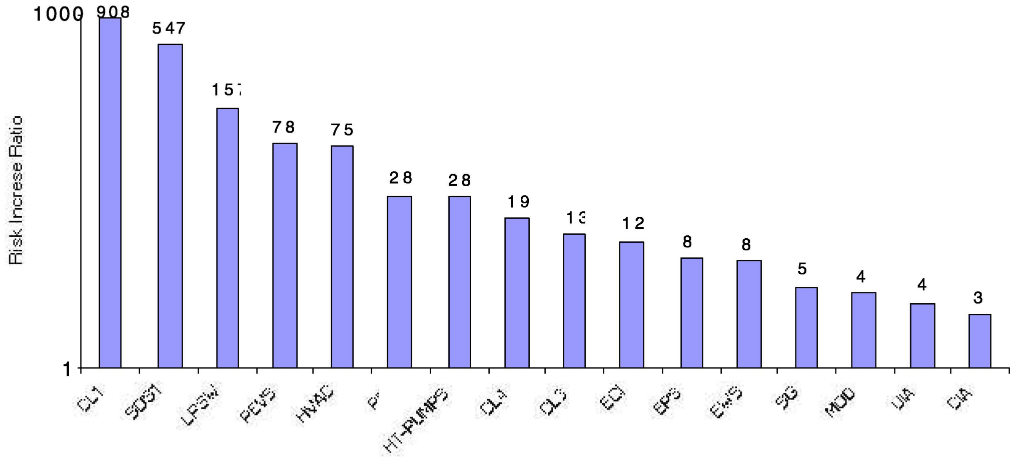
A measure of the importance of various systems to core damage is presented in the bar graph of Figure 4, which shows the factor by which the core damage frequency (sum of FDC1 and FDC2) would increase if various systems were assumed to be in the failed state. From this perspective the Class I system is determined to be the most important. This system provides power to critical control circuits and is normally of very high reliability.

## D. FDCs 3-5

Fuel damage category FDC3 represents those accident sequences in which a loss of ECI occurs either prior to, or during the first hour after, the occurrence of a loss of coolant of intermediate size (initial discharge rate ~100 kg/s) or greater. In these sequences, moderator cooling is successfully provided (otherwise an FDC2 event would result). Accident sequences in which the initiating event is a loss of coolant of small size (initial discharge rate < 40 kg/s), or in which ECI fails in the intermediate (1-24 hours) or long term (> 24 hours), are placed in fuel damage category FDC4 or FDC5. The estimated frequencies of these categories are all of similar magnitude, around 1 x $10^{-4}$ per reactor per year.

## E. FDCs 6-9

These categories possess the common characteristic that they represent the direct outcome of initiating events, with potential radiological consequences even if all mitigation functions as designed. These accident categories



Legend

| | | | |
|---|---|---|---|
| CIA | Common Instrument Air | HVAC | Heating, Ventilation and Air Conditioning |
| CL1 | Class I Power | LPSW | Low Pressure Service Water |
| CL3 | Class III Power | MOD | Moderator |
| CL4 | Class IV Power | PEVS | Powerhouse Emergency Venting |
| ECI | Emergency Coolant Injection | PIC | Pressure and Inventory Control |
| EPS | Emergency Power | SDS1 | Shutdown System No. 1 |
| EWS | Emergency Water | SG | Standby Generators |
| HT-PUMPS | HT Pump Gland Seal LOCA and HT Circulation | UIA | Unit Instrument Air |

FIGURE 4
Risk Significant Systems to Severe Core Damage (At-power)
Mean Frequency: 5.7 x $10^{-5}$ occ/reactor-yr

are unique to pressure tube reactor designs, which give rise to the possibility of accidents involving degraded cooling to fuel in individual channels without impacting the remainder of the core. On-power fuelling increases the opportunity for accidents of this kind.

Fuel damage category FDC6 comprises events in which temporary loss of fuel cooling and consequential limited fuel failure occurs in many fuel channels, prior to successful ECI. For LOCAs with initial discharge rate > 3000 kg/s, fuel failures and fission product release are expected to occur due to rapid voiding of the fuel channels. Therefore, the large LOCA initiating event with successful ECI was conservatively allocated (as the only contributor) to FDC6, which postulates fuel sheath failures in many channels. The frequency of such large LOCAs is expected to be below 1 x $10^{-4}$ per reactor per year.

Accident sequences in fuel damage category FDC7 include single channel failure LOCA events with an initial discharge rate in the range of 40-100 kg/s into the reactor vault. Such events are expected to result in containment isolation (button-up) by either high radioactivity or high reactor vault pressure signal. The estimated frequency is 3.5 x $10^{-4}$ per reactor per year.

Accident sequences in fuel damage category FDC8 include single channel failure events with an initial discharge rate of less than 40 kg/s into the reactor vault. The estimated frequency is 4.7 x $10^{-3}$ per reactor per year.

Events in FDC9, the final category in the fuel damage categorization scheme, in reality do not lead to any fuel damage. All that they result in is the initiation of ECI in order to prevent fuel damage. However, there are significant economic penalties associated with ECI initiation due to the downgrading of the heavy water coolant and due to the loss of power generation during repairs. The estimated frequency is 2.5 x $10^{-2}$ per reactor per year or approximately once every 40 reactor-years.

## IV. EX-PLANT RELEASE CATEGORIES

The BBRA Study established 10 categories of off-site releases to encompass the risk from all possible levels of radioactivity release to the public (see Table 2).

Similar to the Fuel Damage Category results, steam and feedwater line break events are significant contributors to EPRCs. As core damage occurs in these sequences partly due to loss of both low pressure service water and emergency water systems, vault cooler failure occurs coincidentally. Random failure of any of the numerous airlocks in any of the four reactor units or the common portion of the containment envelope leads to a pathway outside containment and, hence, a fission product release.

In addition to impacting vault cooler operation as discussed above, secondary side breaks can also increase the probability of containment isolation failure due to any inadequacies in environmental qualification of containment isolation equipment. They can also contribute to loss of containment integrity by causing a loss of instrument air, normally used to keep the airlock seals inflated, thereby placing a demand on backup air supplies via local air reservoirs in the short term and operator action to valve in a nitrogen supply to keep the air lock seals inflated in the longer term.

Containment may be bypassed in some core damage events due to HT coolant being discharged to outside containment due to equipment malfunctions and operator errors when the reactor is operating at power. For example, the loss of coolant may occur via ruptured steam generator tubes, the HT pump seals, or the $D_2O$ storage tank. In such events, the HT system is initially full of water, and there is significant retention of fission products in the HT system to prevent a large fission product release from occurring. A release outside containment can also occur if core damage occurs when the reactor is in the shutdown state with the HT system open outside containment due to maintenance work on the HT pumps as, in this case, containment is breached if the opening cannot be closed.

TABLE 2

Bruce NGS B Ex-Plant Release Category Logic and Frequencies

| EPRC | Characteristics | Frequency (occ/yr) |
|---|---|---|
| 1 | Large early radioactivity release into containment (0 - 24 hours after initiating event);<br>Pre-existing or early consequential containment envelope impairment;<br>Ex-plant release driven by steaming with vault coolers unavailable to mitigate. | 2.8 x $10^{-9}$ |
| 2 | Large delayed release into containment (at least 6 hours after initiating event);<br>Pre-existing containment envelope impairment,<br>Ex-plant release driven by steaming with vault coolers unavailable to mitigate. | 9.1 x $10^{-8}$ |
| 3 | Significant early release into containment (0 – 24 hours after initiating event);<br>Pre-existing containment envelope impairment;<br>Ex-plant release driven by steaming mitigated by vault coolers. | 2.7 x $10^{-8}$ |

TABLE 2

Bruce NGS B Ex-Plant Release Category Logic and Frequencies

| EPRC | Characteristics | Frequency (occ/yr) |
|---|---|---|
| 4 | Significant delayed release into containment (at least 6 hours after initiating event);<br>Pre-existing containment envelope impairment;<br>Ex-plant release driven by steaming mitigated by vault coolers.<br>*Or,*<br>Significant delayed release into containment (at least 6 hours after initiating event);<br>Late containment failure due to steam-pressurization;<br>Ex-plant release driven by steaming with vault coolers unavailable to mitigate. | $6.9 \times 10^{-8}$ |
| 5 | Large delayed release into containment (> 24 hours after initiating event);<br>Pre-existing containment envelope impairment;<br>Ex-plant release driven by steaming with vault coolers unavailable to mitigate. | $2.0 \times 10^{-10}$ |
| 6 | Significant delayed release into containment (> 24 hours after initiating event);<br>Pre-existing containment envelope impairment;<br>Ex-plant release driven by steaming mitigated by vault coolers.<br>*Or,*<br>Significant delayed release into containment (> 24 hours after initiating event);<br>Late containment failure due to steam-pressurization;<br>Ex-plant release driven by steaming with vault coolers unavailable to mitigate. | $1.8 \times 10^{-7}$ |
| 7 | Small release from containment bypass, such as HT pump gland seal failure, boiler tube rupture, ECI blowback, pipe break in $D_2O$ feed/bleed system of LOCA2A size outside containment;<br>Ex-plant release via direct path-way outside containment. | $3.5 \times 10^{-6}$ |
| 8 | Significant early release into containment due to failure of reactor shutdown;<br>Pre-existing or early consequential containment envelope impairment (containment envelope crack due to over-pressure by steam surge);<br>Early short-term ex-plant puff-release. | $4.7 \times 10^{-10}$ |
| 9 | Design basis fuel failure events (large LOCA, single channel events with containment pressurization, LOCA*ECI and LOCA*ECR, moderator heat sink available);<br>Early ex-plant release due to containment bypass with failure of boiler SRV cooldown, or depleted containment vacuum and pre-existing containment envelope impairment. | $5.9 \times 10^{-6}$ |
| 10 | Design basis fuel failure events (see EPRC9);<br>Intact containment and all containment systems available;<br>Delayed noble gas release via EFADS (> 24 hours after initiating event). | $5.8 \times 10^{-5}$ |

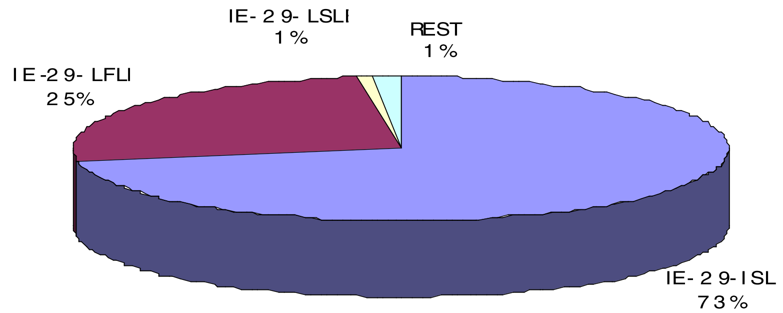


FIGURE 5
IE Contribution to EPRC2 (At-power)
Mean Frequency: 7.7 x $10^{-8}$ occ/reactor-yr

The initiating events that are key contributors to the occurrences of a release outside containment may be inferred from a review of one of the important EPRCs. EPRC2 is chosen here based on its calculated frequency and the nature of events in this category. EPRC2 contains total loss of heat sink sequences leading to severe core damage due to failure of the normal and backup heat sinks with coincident breach of containment (e.g., airlock service side door seals deflated), and small LOCAs with ECI and moderator failure with coincident breach of containment and failure of vault coolers. EPRC2 is also chosen because it is a dominant contributor to the individual early fatality frequency. Figure 5 shows the initiating event contributions to EPRC2. High energy pipe break events such as steam and feedwater line breaks dominate due to their contribution to both the occurrence of core damage and impact on containment systems.

## V. ACCIDENT CONSEQUENCE AND RISK

The primary consequence and risk estimates generated by the Study are given in Tables 3, 4, and 5. The fuel damage categories (FDCs) by themselves only cause internal economic impacts and it is not until some radioactivity is released to the environment that public risk becomes a consideration. Off-site risk is associated with the ex-plant release categories (EPRCs).

Table 3 represents the accident-related financial consequences and risk of operating a multi-unit station, where an accident at one unit has a direct impact on the operability of the other units. The dominant contributors by a large margin are the two most probable but lowest consequence FDCs 8-9. This is because there is a substantial cost associated with any accident sequence that involves actuation of ECI caused by the requirement to shut down all units, independent of whether there is any fuel damage. The need to recover $D_2O$ from ECI water, re-poise safety systems, and repair, inspect and refill the HT system contribute to the length of the resulting outage and associated loss of production which determines the consequence.

Table 4 contains the off-site consequence estimates associated with the accidents represented by the EPRCs. In the case of individual dose at the site boundary, results in the non-stochastic range (assumed to be greater than 3 Sv) are not reported but simply assumed to lead to individual early fatality. An economic equivalent for dose was obtained by assigning a value of $400,000 per Person-Sv. Property damage includes losses due to land use interdiction, loss of economic activity, costs of population relocation, etc.

TABLE 3
Fuel Damage Category
Mean Economic Risk Estimates

| FDC | Mean Frequency<br>(/yr) | Mean Consequence<br>(Million $) | Mean Risk<br>(M$/yr) |
|---|---|---|---|
| 1 | 6.0 x $10^{-8}$ | 10,400 | 6.2 x $10^{-4}$ |
| 2 | 6.4 x $10^{-5}$ | 10,400 | 6.7 x $10^{-1}$ |
| 3 | 9.5 x $10^{-5}$ | 6,560 | 6.2 x $10^{-1}$ |
| 4 | 9.3 x $10^{-5}$ | 6,560 | 6.1 x $10^{-1}$ |
| 5 | 1.5 x $10^{-4}$ | 2,630 | 4.0 x $10^{-1}$ |
| 6 | 1.0 x $10^{-4}$ | 2,630 | 2.6 x $10^{-1}$ |
| 7 | 3.5 x $10^{-4}$ | 1,265 | 4.4 x $10^{-1}$ |
| 8 | 4.7 x $10^{-3}$ | 1,265 | 6.0 x $10^{0}$ |
| 9 | 2.5 x $10^{-2}$ | 460 | 1.2 x $10^{1}$ |
| Total risk (1 unit) | | | 2.1 x $10^{1}$ |
| Total risk (4 units) | | | 8.4 x $10^{1}$ |

TABLE 4
Ex-Plant Release Category Mean Consequence Estimates

| EPRC | Individual Dose*<br>(Sv) | Population Dose**<br>(P-Sv) | Health-related Economic Consequences<br>($ Million) | Property Damage Economic Consequences<br>($ Million) |
|---|---|---|---|---|
| 1 | >3 | 32,900 | 13,200 | 1,370 |
| 2 | >3 | 35,400 | 14,200 | 1,850 |
| 3 | >3 | 10,400 | 4,200 | 509 |
| 4 | >3 | 8,730 | 3,500 | 440 |
| 5 | 0.26*** | 22,700 | 9,100 | 799 |
| 6 | 3.0 | 2,800 | 1,100 | 21 |
| 7 | 0.59 | 760 | 300 | 1 |
| 8 | 0.22 | 40 | 16 | 0 |
| 9 | 0.27 | 240 | 100 | 0 |
| 10 | 0.037 | 7 | 3 | 0 |

* At assumed site boundary of 1 km

** Out to 200 km radius from site, total population 6.5 million

*** Evacuation during emergency phase credited because release is delayed >24 hours

Table 5 summarizes the individual health and overall economic risks associated with accidents represented by the EPRCs. The totals represent the risk from one unit and the four-unit station. Categories that contribute to individual early fatality are not included as contributors to individual delayed fatality to avoid double-counting.

TABLE 5
Mean Individual Risk Estimates for EPRCs

| EPRC | Mean Frequency (/yr) | Individual Early Fatality Risk (/yr) | Individual Delayed Fatality Risk (/yr) | Offsite Economic Risk ($/yr) | | |
|---|---|---|---|---|---|---|
| | | | | Health-related | Property Damage | Total |
| 1 | 2.8 x $10^{-9}$ | 2.8 x $10^{-9}$ | N/a | 37 | 4 | 41 |
| 2 | 9.1 x $10^{-8}$ | 9.1 x $10^{-8}$ | N/a | 1300 | 170 | 1,470 |
| 3 | 2.7 x $10^{-8}$ | 2.7 x $10^{-8}$ | N/a | 110 | 14 | 124 |
| 4 | 6.9 x $10^{-8}$ | 6.9 x $10^{-8}$ | N/a | 240 | 30 | 270 |
| 5 | 2.0 x $10^{-10}$ | 0 | 2.6 x $10^{-12}$ | 2 | 1 | 3 |
| 6 | 1.8 x $10^{-7}$ | 0 | 2.7 x $10^{-8}$ | 200 | 4 | 204 |
| 7 | 3.5 x $10^{-6}$ | 0 | 1.1 x $10^{-7}$ | 1100 | 4 | 1,104 |
| 8 | 4.7 x $10^{-10}$ | 0 | 5.2 x $10^{-12}$ | ~0 | 0 | ~0 |
| 9 | 5.9 x $10^{-6}$ | 0 | 8.3 x $10^{-8}$ | 590 | 0 | 590 |
| 10 | 5.8 x $10^{-5}$ | 0 | 1.1 x $10^{-7}$ | 170 | 0 | 170 |
| Total (1 Unit): | | 1.9 x $10^{-7}$ | 3.3 x $10^{-7}$ | 3,800 | 230 | 4,030 |
| Total (4 Units): | | 7.6 x $10^{-7}$ | 1.3 x $10^{-6}$ | 15,200 | 920 | 16,120 |

TABLE 6
Relationship Between BBRA Consequence Categories and Safety Goals

| Safety Goal | Basis for Implementation | Relationship To BBRA Consequence Categories |
|---|---|---|
| Severe Core Damage Frequency<br>(per unit) | Core disassembly | ΣFDC1-2 |
| Individual Early Fatality Frequency (per site) | Individual dose at site boundary > 3 Sv | 4 x ΣEPRC1-4 |
| Individual Delayed Fatality Frequency<br>(per site) | Frequency x individual dose x radiation risk factor | 4 x (individual risk summed over EPRC6-10) |
| Large Release Frequency (per unit) | Fraction of cesium-137 (Cs-137) released from containment > 1% | ΣEPRC 1-6 |
| Severe Release Frequency<br>(per unit) | Fraction of Cs-137 released from containment > 10% | ΣEPRC 1-3, 5 |

## VI. SUMMARY OF RESULTS

The results of BBRA were also compared against OPG risk-based safety goals. The relationship between these goal and FDCs/EPRCs is shown in Table 6.

Table 7 provides a comparison of the numerical results of BBRA against the OPG,N risk-based safety goals. The Bruce NGS B severe accident frequency of 6.4 x $10^{-5}$ per reactor per year falls below the limit but above the target. The implication is that specific action should be taken to identify if there are cost-effective ways to further reduce this frequency. Design changes and improvement initiatives are already underway to achieve a reduction in the frequency. Calculated values for early fatality & delayed fatality fall below the goals and no further action is warranted. The goals themselves are derived from the criterion that the additional risk to any individual from operation of a nuclear site should not result in an increase in the corresponding background risk of more than 1 per cent. The BBRA results fall well below the goals, so the actual increase is much less than 1 per cent. The calculated large release frequency is below the relevant goal and the severe release frequency is only marginally above its goal. No further action to reduce these frequencies is warranted.

TABLE 7
Comparison of BBRA Results with Ontario Power Generation Nuclear Safety Goals

| Safety Goal<br>(application) | Risk Limit<br>(per year) | Risk Target<br>(per year) | Calculated Risk<br>(per year) |
|---|---|---|---|
| Severe Core Damage (per unit) | $10^{-4}$ | $10^{-5}$ | 6.4 x $10^{-5}$ |
| Early Fatality * (per site) | $10^{-5}$ | $10^{-6}$ | 7.7 x $10^{-7}$ |
| Delayed Fatality * (per site) | $10^{-4}$ | $10^{-5}$ | 2.6 x $10^{-6}$ |
| Large Off-Site Release (per unit) | $10^{-5}$ | $10^{-6}$ | 3.7 x $10^{-7}$ |
| Severe Off-Site Release (per unit) | $10^{-6}$ | $10^{-7}$ | 1.2 x $10^{-7}$ |

* at site boundary (1 km)

## VII. PLANT IMPROVEMENTS

The BBRA Study has determined that the Bruce NGS B station, as designed and operated, does not lead to any significant risk to the public, and meets the Ontario Hydro safety limits. It is implicit in the assumptions of the BBRA Study that the plant's analyzed design basis is maintained, actual component failure rates are not substantially higher than indicated in the BBRA data base, and operating practices and operator training are such that the assumptions used to generate human error probabilities remain valid.

Improvement initiatives currently underway in OPG,N to correct the recent decline in performance and re-establish the design basis, restore configuration control, improve component reliability, reduce maintenance backlogs, and improve staff training are assumed to have been effectively implemented. It is, therefore, implied that further design or operational changes to Bruce NGS B are warranted only if they are cost-effective. With improvements to the powerhouse emergency venting installed, the Environmental Qualification program implemented, and the ability of the operator to recover from failed equipment enhanced, the core damage frequency is expected to be reduced to near the target value of 1 x $10^{-5}$ per reactor per year. Other potential plant improvements are identified in the BBRA main report [3].

During the fault tree analysis phase of the Study, a number of observations were made with respect to plant design and operation. Some of the observations resulted in operational changes, such as more frequent testing of certain circuit breakers to confirm their operability, and check valves to confirm prevention of back-flow.

## VIII. BBRA APPLICATIONS

The BBRA models have been used frequently in assessing the safety impact of abnormal configuration changes such as out-of-service equipment, design changes, deferred testing, and safety analysis findings. The BBRA models have also formed the basis of the unavailability models required by the licensing process. Some of the recent examples of BBRA based assessments are:

- assessment of risk associated with the use of adjuster rods;
- risk impact of reactor regulating system (RRS) design changes;
- time-at-risk assessments for the short term use of seismically non-qualified equipment;
- shutdown strategy assessment in response to group 2 impairment;
- risk impact of HT pressure & inventory control (PIC) design changes;
- electrical distribution system (EDS) assessment;
- risk impact of postponing SDS2/ECI SSTs due to DC converter outage;
- risk impact of boiler divider plate failure;
- development of critical component lists;
- development of outage model; and
- development of on-line model

OPG,N has already utilized the BBRA models on the R&R Workstation tool called EOOS (Equipment Out-Of-Service) for outage configuration assessment by station staff, using one of the fastest minimal cutset solution engines called RSAT (Risk Spectrum Analysis Tool) in what is believed to be the first application of RSAT within the EOOS environment.

The process to obtain EOOS models from the BBRA fault trees, developed on OPG's IBM SP machine running under UNIX, has been stream-lined and was recently used to implement an on-line risk monitoring tool at Bruce B. The following are some features of this process:

- In the BBRA, models for some system failure events were developed in the form of Boolean equations, using the SETS code [4], rather than explicit fault trees to take advantage of their similarity with those events for which fault trees were available. As an example, fault trees were explicitly drawn for only 8 representative 48v d.c. power supplies. Models for the remaining 29 were derived directly from the cutsets of the 8 representative buses with significant labour savings, but without any loss of accuracy. Logic models for the numerous room ventilation and air-conditioning systems were similarly developed. However, EOOS implementation requires that all logic models be available in the form of fault trees, from which a single overall fault tree is developed for the consequence category of interest. A number of UNIX scripts were developed to automatically derive the required fault trees, using the relational information set up to obtain the Boolean equations.

- A difficulty with assembling the system fault trees in the form of a single fault tree is that the resulting fault tree may contain logic loops. As an example, the fault tree for loss of low pressure service water (LPSW) system (event A, say) contains the loss of unit instrument air (event B, say) as a contributor. This arises, e.g., due to the possibility of LPSW flow diversion away from critical loads on loss of unit instrument air. Loss of unit instrument air, in turn, can occur if the air compressors fail. A contributory cause of failure of the air compressors is, however, loss of LPSW itself due to failure to provide compressor cooling. Hence, a logic loop results. Fault tree codes, in general, fail when logic loops are encountered.

  To break a logic loop one needs to re-define event B (say, to event B-NEW) solely for use in the fault tree for event A, with event A removed. In the BBRA, this was achieved easily via a step in a SETS user program that directly modified the equation for event B. The equation for B-NEW was then used in obtaining the equation for event A. This equation for event A is then substituted into the equation for event B to obtain a solution for event B for use in evaluating other fault tree top events than A that are dependent on event B. For EOOS implementation, however, the fault tree for event B needs to be additionally re-cast in a form with B-NEW as the top event. Again, UNIX scripts were written and executed to automatically generate the required new fault trees based on knowledge of loop cutting logic contained in the SETS user programs.

## IX. CONCLUSIONS

The principal conclusions of the Study are:

(a) The risk to the health and welfare of the population living or working in the vicinity of the Bruce Nuclear Power Development from the operation of Bruce NGS B is significantly lower than other risks to which they are normally exposed. The mean individual public health risks are below the Ontario Power Generation, Nuclear (OPG,N) safety goals.

(b) The likelihood of an accident causing severe damage to the reactor core is acceptably low and similar to that calculated for other contemporary reactor designs. The calculated mean frequency for severe core damage falls above the OPG,N safety goal, but is within the range of acceptability. The calculated frequency is similar to that for peer plants in the United States and is less than that estimated for the older Pickering NGS A, but is higher than that for more recent CANDU reactors such as Darlington NGS. This latter finding is largely due to the more limited capability of Bruce NGS B safety-related systems to survive in a hostile powerhouse environment.

(c) The likelihood of an accidental release large enough to warrant relocation of members of the public is sufficiently low that it can be considered negligible for all practical purposes.

(d) External economic risks from the accidental release of airborne radioactivity off-site are low. The internal business risk to Ontario Power Generation from an accident is quite large, but typical for OPG,N multi-unit stations with shared safety systems, with the dominant contribution arising from the relatively more likely, low consequence events.

The calculated results exceed safety goals in two areas; severe core damage frequency and severe release frequency, but no safety limits are exceeded. It is expected that with the anticipated design changes, and with the improvement initiatives currently underway (design basis re-established, configuration control restored, component reliability improved, maintenance backlogs reduced, staff training improved), both these risk indicators will approach their respective goals.

## REFERENCES

1. Probabilistic Risk Assessment Policy, N-POL-RA-0014, Revision 00, Ontario Power Generation, Nuclear, June 9, 1999.

2. A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, NUREG/CR-2300, Volume 1, U.S. Nuclear Regulatory Commission, January 1983.

3. Bruce NGS B Risk Assessment Main Report, NED Report No. NK29-03611-985088, January 1999.

4. Worrell, R.B., SETS Reference Manual NUREG/CR-4213, US Nuclear Regulatory Commission, Washington DC, May 1985.