EVALUATION OF SEVERE ACCIDENT RISK IN THE PICKERING A RISK ASSESSMENT

K.S. Dinnie and V.M. Raina
Risk Assessment Section
Reactor Safety and Operational Analysis Department
Nuclear Technology Services Division
Ontario Hydro

1 INTRODUCTION

The nature of the design of commercial power plants is such that significant impacts on public health can only occur if a number of barriers fail. Rigorous design and licensing requirements ensure that the more likely accidents do not fail all these barriers and their contribution to risk is likely to be small. The task of estimating accident risk must, therefore, focus more towards those less likely but potentially more serious combinations of failures that are characterized by the following;

a) a large release of fission products into the containment atmosphere,
b) a breach in the containment envelope, and
c) the existence of a driving force to expel the containment atmosphere to the outside environment.

The likelihood of such conditions existing simultaneously during the course of an accident is expected to be small, such that experience and data regarding the behaviour of plant systems under such conditions is sparse or non-existent. The challenge of Probabilistic Safety Assessments (PSAs) is to examine the potential for severe accidents using approaches that are sufficiently detailed and realistic to provide valid information regarding plant risk and susceptibilities, while simple enough to keep the analysis manageable.

This paper outlines the key features of the Pickering A Risk Assessment (PARA) [1] and the manner in which it addresses these issues, and provides some insights into the results and conclusions drawn from the study.

2 STRUCTURE OF THE PARA

A major task in the Pickering A Risk Assessment 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 magnitude of the associated release. As the number of such possible accident sequences is potentially large it is not feasible to explicitly calculate the consequences of each one of them. Instead, it is

customary in PSAs to group events by similarity of the expected radionuclide release. Risk assessments achieve this by first defining *categories* of releases of radioactivity, encompassing the possible range of releases with the potential for significant health consequences, and then allocating all the various event sequences to one of these release categories. It is the accident categories that form the structure of the PSA, providing the link between accident frequency estimates and accident consequence estimates to generate estimates of risk.

Categorization serves as a means to ensure the full range of potential consequences is addressed and as a vehicle to ensure that the study is complete within its defined scope by requiring that all identified sequences be assigned to a category, unless designated as insignificant to risk. It is this requirement for *completeness* that is the essential characteristic of PSA and, at the same time, its greatest challenge.

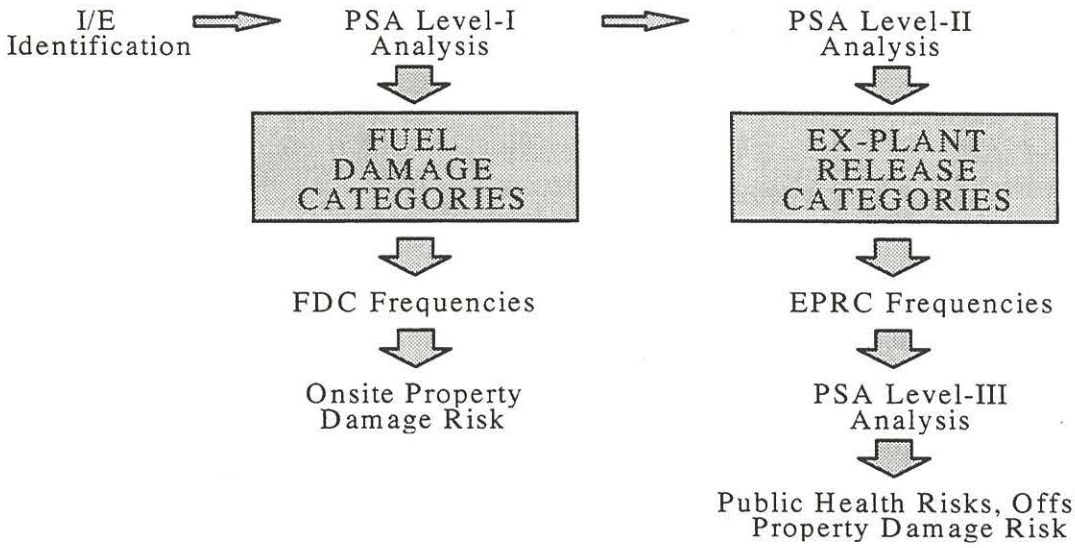
The process of consequence categorization is intimately affected by the interplay between design and operation of plant systems, equipment configuration, plant response to various malfunctions, and understanding of the physical processes that take place inside the reactor and containment when plant systems fail. The complexity of reactor design, operation, and the often uncertain state of knowledge of plant response to various accidents makes it necessary to adopt a structured approach to categorization, while at the same time retaining the flexibility of being able to iterate on the definitions as more information is obtained.

The PARA utilized two broad categorization schemes. The first had as its primary objective the characterization of accident sequences by the extent of the resulting fuel damage, with the output being a set of so-called *Fuel Damage Categories* (FDCs). Fuel Damage Categories were defined to the extent possible on the basis of existing design basis accident analysis, as documented in the plant's safety report. The second took account of the behaviour of containment systems given the occurrence of fuel damage inside containment, leading to a set of categories based on magnitude and timing of release to the environment.

Knowledge of the consequences of design basis events is insufficient to enable the development of such a categorization scheme since they usually span only a narrow band of the possible set of consequences, the intent of design basis analysis being to demonstrate low consequences for design basis events. Hence, analyses were undertaken to assess the consequences of combinations of fuel damage events and containment subsystem failures not assessed in the safety report, on which was based the development of so-called *Ex-Plant Release Categories* (EPRCs). As the purpose of these analyses is to develop broad consequence categories and enable the allocation of accident sequences to them, rather than to assess compliance with narrowly-defined licensing limits, the required level of rigour in such analysis is less than in traditional licensing analysis.

In PSA parlance, the development of the analysis to the point of fuel damage categories is called the *Level-I* analysis, the ex-plant release categories the *Level-II* analysis and the

Figure 1:
The Structure of the PARA



offsite consequence and risk the *Level-III* analysis. The structure of the PARA is shown graphically in Figure 1.

3 THE PARA RISK MODEL

Products of the PARA included; lists of accident sequences belonging to each FDC and EPRC, the frequency of occurrence of each accident sequence and category, and the health and economic consequences associated with each category. Such outputs afford the opportunity to determine the impact on accident frequency and consequence, and hence risk, if changes occur to plant design and operation. This set of outputs is referred to as a *risk model.*

The PARA risk model may be described in terms of its following elements:

1. Definitions of Fuel Damage Categories
2. Identification of event sequences leading to the various FDCs
3. Dominant contributors to each FDC
4. Items similar to 1 and 3 for Ex-Plant Release Categories.

The following deals with the Level-I component of the PARA.

3.1 Fuel Damage Categories

Based on a knowledge of Pickering A's engineered systems, safety features, and an understanding of plant response to accidents documented in the safety report, events leading to fuel damage were classified into nine categories, as shown in Table 1.

A distinction was drawn between events affecting fuel in a single channel (FDC7/8) and those potentially affecting the whole core. With the exception of a large loss-of-coolant-accident (FDC6), damage to fuel in the core requires impairment of Emergency Coolant Injection (ECI) and the magnitude of the damage depends largely on when after shutdown the requirement for ECI occurs (FDC3/4/5). Finally, sequences leading to core disassembly were divided into two categories; *rapid* (FDC1), resulting from failure to shutdown and *slow* (FDC2), from loss of all heat removal. A ninth category was added to reflect the economic penalty arising from the consequences of ECI injection (FDC9), such as a prolonged multi-unit outage.

FDC1 and FDC2 constitute the *severe accident* categories, those involving failures leading to loss of the core structural integrity. Such events intrinsically present a much greater hazard potential, because of the massive degree of fuel damage and greater challenge to containment systems. Sequences involving loss of primary heat sink leading to the potential for consequential multiple fuel channel failures were allocated to FDC4, based on a judgement that overall core structural integrity would be maintained, even though such events are normally considered to be beyond the design basis.

3.2 Event Sequence Identification

An event in a fuel damage category occurs if normal reactor operation is somehow interrupted and mitigation of the effects of such an interruption fail. Identification of accident sequences, therefore, requires determination of various ways by which normal operation can be upset, identification of the available mitigating systems if any, and an assessment of the abilities of mitigating systems to cope with the upset. These three requirements are met in a risk assessment by carrying out the tasks of initiating event selection, event tree analysis and fault tree analysis.

Fault tree analysis was the primary vehicle for the quantification of event sequence frequencies and formed a major activity of the total risk assessment effort. First the high level logic for each FDC derived from the event trees was captured in the form of what is called the fuel damage category logic, which in itself is a fault tree representation of the constituents of each FDC. Then fault trees were developed for each of the mitigating systems appearing in the FDC logic. A similar exercise is conducted with respect to the ex-plant release categories, giving rise to what is called the EPRC logic.

The Pickering NGS A risk model contains fairly detailed fault tree models for 34 plant systems. Each of these plant models contains all relevant information about the given system's topology, interactions with other systems, control aspects, operator/maintainer interface, capability, test and maintenance policies and records, and response to initiating events. The resulting fault tree logic and data files, thus, are an archive of information about the system's safety function.

Table 1
Frequency of Fuel Damage Categories

FDC	Description	Mean Frequency (occ/yr)
FDC1	Failure to shut down following fast loss of power regulation	5×10^{-7}
FDC2	LOCA and failure of emergency coolant injection and moderator heatsink	1.3×10^{-4}
FDC3	LOCA and failure of high pressure emergency coolant injection	7×10^{-6}
FDC4	LOCA and failure of emergency coolant recovery	1×10^{-5}
FDC5	Small LOCA and failure of emergency coolant recovery	4×10^{-5}
FDC6	Large LOCA with extensive fuel failures	2×10^{-5}
FDC7	LOCA resulting in fuel failures in one channel and containment pressurization	7×10^{-4}
FDC8	LOCA resulting in fuel failures in one channel but without containment pressurization	7×10^{-3}
FDC9	LOCA requiring emergency coolant injection	2.6×10^{-2}

The category logic and the system fault trees were then logically integrated by means of computer methods, supported by component failure data bases, and operator reliability quantification models to generate lists of so-called minimal cutsets, representing the most likely, or dominant, ways by which each category of events can occur.

3.3 Dominant Contributors to Severe Core Damage Accidents

Estimated frequencies for the nine FDCs are given in Table 1. The severe core damage frequency for a Pickering A reactor was calculated in the PARA to be 1.3×10^{-4} per year (the sum of FDC1 and FDC2), resulting primarily from event sequences in which a loss of coolant occurs, initiated by a pipe break in the heat transport system or induced by a transient event, followed by failure in the longer term of the D_2O recovery system, the emergency coolant injection system and the moderator heat sink. A common theme in these accident sequences was the presence of design features that lead to dependencies between the various mitigating systems and initiating events. A few of the dominant accident sequences and underlying dependencies are discussed below.

(a) In the event of a LOCA at Pickering A, following successful completion of the initial injection phase, the emergency coolant recovery (ECR) function is implemented by the use of the moderator system pumps to recover and pump back the water escaping from the HT system break and accumulating in the reactor building sumps. Should these pumps fail, both the emergency coolant recovery (ECR) function and the moderator heat sink

function, therefore, fail. Unique design features, and failure criteria derived from the station's Safety Report, make the pumps vulnerable to a number of single failures. For example, failure of the dump port level controller or loss of air supply to the calandria outlet valves (COVs) leads to the moderator pumps gas-locking, loss of a single Class III power bus causes enough pumps to fail to lead to insufficient flow, failure of a control power bus leads to loss of all moderator room air cooling units, and the spurious opening of an air-operated sump isolation valve leads to the moderator pumps being aligned to the sumps soon after the LOCA when the latter are empty.

(b) Transient events have the potential to cause a loss of coolant as well as failure to mitigate the LOCA in the longer term by means of the moderator pumps. An example of such an event is the loss of air supply to the reactor building which may also lead to the heat transport relief valves opening and, in conjunction with bleed condenser relief valves failing to reclose, to a LOCA, as well as failure to open the D_2O recovery isolation valve. Failure of the moderator pumps due to gas-locking initiated by COVs failing open on loss of the air supply then leads to core damage. Many of these failures, however, are recoverable before core damage occurs.

(c) Dependencies also exist between the various heat removal systems. Among these are the reliance of main and auxiliary boiler feedwater and shutdown cooling on common Class IV and III power supplies, and common low pressure service water (LPSW) supplies. Steam line breaks, condenser cooling water (CCW) line breaks and service water line breaks in the power house have the potential to cause widespread loss of electrical, instrument air and cooling water supplies, thereby affecting a number of heat removal systems. Steam line breaks can not only lead to loss of the class III and IV power supplies but also the power supplies required to open the ECI motorized valves.

(d) The operation of a number of backup or protective systems can be defeated due to the reliance on the operator to initiate them. An example is the provision of an alternate heat sink after loss of normal main feedwater supply, the multiplicity of backup cooling systems such as auxiliary feedwater, shutdown cooling, and emergency boiler water systems notwithstanding. In fact, the PARA results indicate that appropriate operator action is a key factor in keeping the core damage frequency low. Other examples of key operator actions are: the throttling of dump tank isolation valves to prevent moderator pump gas-locking, initiation of ECI following a very small LOCA as boiler room pressure may not rise sufficiently for automatic initiation to occur; isolation of condenser cooling water pipe breaks to prevent water levels in the powerhouse basement from reaching such heights that the instrument air systems fail, startup of the emergency LPSW pumps following a loss of main LPSW pumps, and the manual energization of Class III buses following failure of the emergency transfer scheme (ETS) to initiate automatically. Timely operator action to trip HT main circulating pumps is an important defence against HT pump seal LOCAs.

(e) A noteworthy feature of the Pickering NGS A design is the availability of auxiliary services from the non-accident units to assist the accident unit. This is either because of

intended redundancy or because of a common shared function which nevertheless can be supplied services from different units. Prime examples of these are the electrical supplies to the HPECI pumps and valves, which can be obtained from either the grid or any non-accident unit on site, the high pressure service water supply from Pickering NGS B Units 6 and 7 to any of the Pickering NGS A units to provide emergency boiler cooling water, the Class III inter-station transfer bus, the paired instrument air systems, and the standby generators. Further, inter-unit ties exist between the instrument air and the low pressure service water systems. The PARA, nevertheless, identified failure modes that affect multiple units. Examples of such failure modes are common grid failures, steam and CCW line breaks, and possible multi-generating unit trips following an initiating event.

3.4 Importance Analysis (Severe Core Damage)

A breakdown of the dominant contributors to severe core damage by type of initiating event is shown in Figure 2. Accident sequences initiated by pipe break LOCAs are found to contribute 83 per cent of the core damage frequency, the rest being contributed by transient initiating events. The contribution of failure to shutdown events (FDC1) to the frequency of core damage was found to be insignificant.

Figure 2 also displays the percentage contribution to severe core damage events of various kinds of LOCAs. Thus, the very small LOCA1 breaks (initial discharge rate within the capacity of D_2O feedpumps, 40 kg/s) contribute 43 per cent, while intermediate breaks (40-1000 kg/s), viz. LOCA2s, account for 26 per cent. The significant contribution of LOCA1 breaks is likely conservative as only a small credit (one chance in four) has been taken for averting core damage through operator action, even though the small leak rate provides considerable opportunity for corrective action.

Of the specially-defined LOCAs, pressure tube failure is the most significant (8 per cent) and all others together total 6 per cent (e.g., large LOCA, stagnation feeder break, flow blockage, steam generator tube rupture).

Figure 2:
Contributors to Severe Core Damage frequency by Event Type

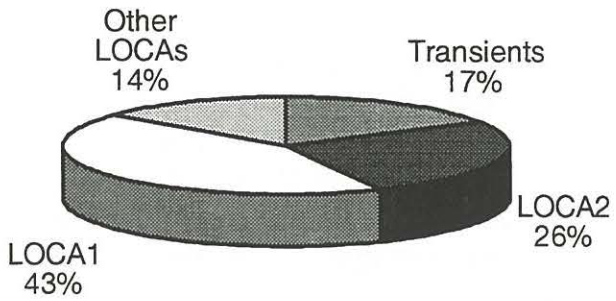
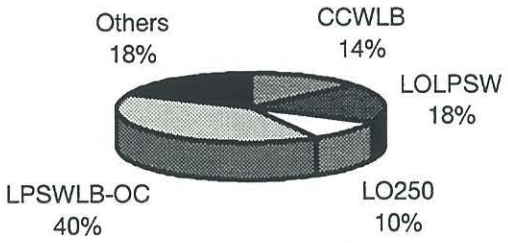


Figure 3:
Breakdown of Transient Initiator Contributors to Severe Core Damage



The overall 17 per cent contribution to severe core damage frequency from non-HT system pipe breaks is broken down in Figure 3. As can be noted, the major contributions arise from losses of service water (LPSWLB-OC, LOLPSW), CCW line breaks (CCWLB) and a 250 V dc electric power bus failure (LO250). Loss of high pressure instrument air (4 per cent of contribution from transients) and large steam line breaks outside containment (3 per cent) are also significant. In general, power supply failure events are relatively low contributors, reflecting a high level of redundancy. In all transient-initiated events, a loss of HT integrity (usually consequential) occurs followed by loss of ECI and moderator heat sink (again usually due to consequential reasons).

An assessment of the importance of the various component failures and human errors giving rise to severe core damage result in the finding that the ability to terminate a small loss of coolant before it develops into core damage is the most important means by which the severe core damage frequency can be controlled, thus pointing to the importance of training in event diagnosis and correction. Improvements in the reliability of the D_2O recovery system, and lowering the chances of moderator pump gaslocking were indicated as being next in importance, followed by that of the moderator sump pumps. Components (or operator actions) which would increase the severe core damage frequency the most if they were assumed to be continuously in the failed state instead of being assigned their expected failure probability, were found to be the shut-off rods, followed by failure of the operator to take action to provide a back-up heat sink.

The frequency of 1.3×10^{-4} per reactor-yr for slow loss of core structural integrity is of the same order of magnitude (within a factor of 2 or so) as the core damage frequency calculated for the majority of the western world's pressurized water reactors (PWRs), to which among all reactor types the Pickering A reactors are the most similar. This is borne out by the numerous PSAs, particularly the Individual Plant Examination (IPE) assessments, carried out recently in the United States. The average US PWR core damage frequency, based on IPEs of 62 reactors, excluding the contribution from the so-called external events and non-power states, is 8.4×10^{-5}/reactor-yr [2], with a range covering about two orders of magnitude, from about 5×10^{-6} to 5×10^{-4}/reactor-yr. Consistent with this, the severe core damage frequency for the more modern Darlington CANDU design was estimated to be 4 x 10-6/reactor-yr [3].

4 SEVERE ACCIDENT CONSEQUENCE ESTIMATION

4.1 Role of Consequence Analysis in PSA

Consequence analysis of nuclear accidents is performed typically using the following process; an accident is identified, the sequence of events (or combination of failures) defined, analysis assumptions developed for the event sequence, and consequence (usually public dose) calculated. This process is repeated for all identified sequences.

In PSA, Level-II (in-plant) consequence analysis is required initially to address two questions; what is the range of consequences that can occur as the result of nuclear accidents and how should the PSA be structured to enable the estimation of the likelihood of occurrence of various levels of consequence over the range of interest? The Level-II analysis must first be used to establish the range of interest, then to simplify the spectrum to a manageable form by establishing suitable discrete consequence categories. Subsequently, a Level-III (offsite) consequence analysis is used to evaluate the dose and economic consequences of accidents representative of the categories.

One outcome of this approach is that accident sequences used in establishing the design basis for the plant and those important in the licensing of the plant may not be important in establishing the risk from the plant. The highly stylized accidents analyzed for licensing are both unlikely, because of the very specific nature of the events and associated assumptions, and of relatively low consequence, because the plant has been designed to ensure the consequences meet strict licensing criteria.

As previously noted, a key product of PSA is the identification of the so-called 'dominant contributors' to risk - the sequences which produce the highest risk contribution. Control of risk requires control of the dominant contributors so it is important to minimize any methodological bias which may artificially increase risk contributions from some sequences at the expense of others. This requires that arbitrary conservatisms be minimized to the extent possible. The broad scope of PSA and state of knowledge of some accident phenomena limits the degree to which conservatisms can be eliminated. The consequence analysis takes an approach which can be summarized as: 'a conservative representation of realistic scenarios'.

Ex-Plant Release Categories. For a significant release of radioactivity to occur from the containment not only must there be a release into the containment building, but there must also exist an opening in the containment envelope and a driving force to expel the radioactive materials through it. The opening could in turn be either *pre-existing* such as isolation failure or leakages through containment penetrations, or be caused by the accident itself, e.g., due to forces resulting from failure to shutdown the reactor, or hydrogen detonation. Furthermore, some core damage events have the potential to bypass containment, such as steam generator tube ruptures and the blowback of heat transport

coolant via the Shutdown Cooling and HPECI valves. The driving force may be provided by inability, due to air cooling unit failure, to condense steam formed as a result of the accident, or a hydrogen burn due to failure of the hydrogen igniters to mitigate the build-up of hydrogen concentrations. Thus, the magnitude and timing of the releases is dependent on the nature of the accident sequence and the state of the containment system.

The lower the accident release and dose, the lower the chance of public health impact and at some point the dose falls below that at which there is a significant chance of any health effects at all. For the PARA this value was set at about 20 P-Sv (total dose to the population within 100 km) and sequences with consequences below this were neglected. The impact on the study was that all sequences resulting in fuel damage inside an intact containment could be excluded, except for severe accidents involving core disassembly.

The EPRC structure was developed based on two fundamental release characteristics which have the greatest influence on accident consequence; timing and magnitude. The timing of the release was categorized into three time bands called *source term periods or STPs*, early (0-6 hours), intermediate (6-24 hours) and late (>24 hours). The magnitude of release was similarly divided in to three bands; large (>> 1% release of core inventory of volatile fission products, principally cesium and iodine isotopes), intermediate (0.1-1% release) and small (< 0.1%). The choice of these boundaries was based partly on scoping analysis and partly on the exercise of reasonable judgement. This 3x3 matrix was used as the conceptual starting point for categorization which eventually led to seven EPRCs being defined (Table 2).

Table 2:
EPRC Structure

Release Timing / Magnitude	Early (STP1)	Intermediate (STP2)	Late (STP3)
Large	EPRC1	EPRC2	EPRC3
Intermediate	EPRC4		
Small	EPRC5/6		EPRC7

Empty cells imply that no sequences with such characteristics were identified or, more likely, that they were conservatively subsumed into more severe categories (i.e., earlier or larger).

The Containment Event Tree. The multi-unit, negative-pressure containment system (NPCS) employed by Ontario Hydro's stations presents a somewhat different challenge to the PSA analyst than single-unit, positive-pressure reactor containment designs. The NPCS contains a number of active sub-systems and components that must be addressed explicitly in the risk model, particularly the vacuum system, air coolers (ACU) and filtered air discharge (FAD). This dictates an event tree/fault tree approach to representing

containment system response rather than the phenomenologically-driven event trees used for the more passive light water reactor (LWR) containments.

The Level-II analysis used to support the development of the containment event tree and EPRCs was one of the major innovations of the PARA. This complex analysis is described elsewhere [4,5]. The results of the analysis indicated that there are few consequential mechanisms that are of sufficient magnitude to challenge containment integrity. The early disassembly of CANDU reactors under severe accident conditions eliminates challenges arising from high-pressure melt ejection from the core and greatly reduces the importance of sequences involving containment bypass. Long-term pressurization is made almost inconceivable by the potential for interconnection of eight reactor buildings and the vacuum building. Only early steam overpressure due to failure to shut down (*ECF*) or the possibility of accumulation of hydrogen in the long term leading to explosive concentrations (*LCF*) were considered credible consequential failure mechanisms.

EPRC Logic. The *EPRC logic* is the name given to the collection of sequences involving in-plant severe accident sequences and containment failure modes, each assigned to the appropriate EPRC based on its release characteristics. The study identified hundreds of such sequences, all of which had to be accounted for by assignment to an EPRC either directly, based on consequence analysis, or indirectly, subsuming the sequence(s) by a more likely combination with similar consequences. The Level-II accident analysis was required to identify the timing and release characteristics of each sequence type for the purposes of allocation to EPRCs.

Each EPRC appears both as a collection of sequences expressed in Boolean logic which can be solved to calculate frequency, and a set of release characteristics which can be modelled in the Level-III consequence code MACCS [6] to calculate public dose and associated economic consequences. The risks are calculated for each category and taken together represent the risk profile for the plant.

4.2 Results of the Consequence Analysis

Dose. Any given set of release characteristics can result in a wide range of dose and economic consequences depending on prevailing meteorological conditions over the course of the release. Results of the consequence calculations are expressed not as a single number but as a probability distribution representing the probability of occurrence of any given level of dose conditional on the occurrence of an event in the EPRC under evaluation. This distribution is best understood when expressed as a *complementary cumulative distribution function* (CCDF), which expresses the probability with which any given level of dose would be *exceeded*, given the occurrence of an event in that EPRC. Typical Level-III analysis results for PARA EPRCs are shown in Figure 4 with mean values given in Table 3.

Historically, economic and social consequences of accidents have proven to be of greater significance than the health consequences. Accident consequence codes have the capability to estimate the dose and cost components associated with the implementation of dose *countermeasures*. Countermeasures imposed to limit the long-term dose consequences of accidents (e.g., evacuation, relocation, decontamination and food interdiction) have significant costs which increase as the contribution to dose decreases.

Economic. The MACCS code incorporates the effect of long-term countermeasures based on projected dose using a user-supplied *intervention dose* criterion, above which countermeasures are taken and below which they are not. The intervention dose is the estimated dose over the first year after the accident (assuming no countermeasures) and is calculated for every sector in the spatial grid used to represent population distribution. The code then uses the dose criterion to determine where countermeasures will be needed and calculates population dose and countermeasure costs accordingly.

The effect of varying the intervention dose criterion on PARA economic consequence results is illustrated in Tables 3 and 4. The results show that, although it is possible to control post-accident dose to a degree, there is a significant cost to achieve only modest reductions (although the relative benefits are masked to a certain degree because no early countermeasures were credited in the analysis leading to an overestimate of the early component of dose).

Figure 4:
Conditional Population Dose CCDFs

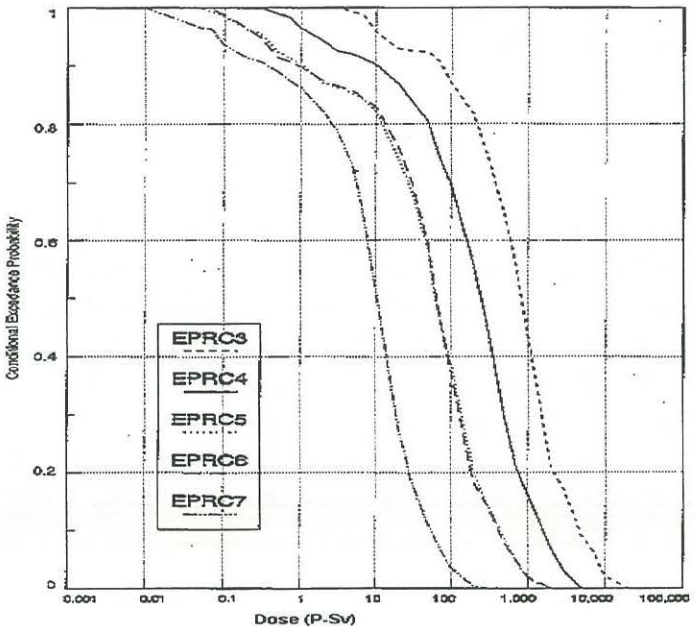


Table 3:
EPRC Mean Dose Consequences v. Intervention Dose

Intervention Dose Criterion (Sv)	EPRC3 (P-Sv)	EPRC4 (P-Sv)	EPRC5 (P-Sv)	EPRC6 (P-Sv)	EPRC7 (P-Sv)
0.005	6.3×10^3	4.6×10^3	8.8×10^2	4.3×10^2	2.1×10^1
0.02	9.7×10^3	6.0×10^3	9.4×10^2	4.9×10^2	2.1×10^1
0.1	1.5×10^4	7.0×10^3	9.4×10^2	5.3×10^2	2.1×10^1

Table 4:
EPRC Mean Economic Consequences v. Intervention Dose

Intervention Dose Criterion (Sv)	EPRC3 $ Million	EPRC4 $ Million	EPRC5 $ Million	EPRC6 $ Million	EPRC7 $ Million
0.005	6000	1300	40	13	0
0.02	2500	280	4	18	0
0.1	535	31	0.2	0.8	0

4.3 Results of the EPRC Frequency Analysis

Results for the frequency of the seven EPRCs are given in Table 5.

Dominant Contributors to Ex-plant Release Categories. The dominant event sequences making up the EPRCs again arise from dependencies between systems that may be implicated in a core damage event and containment subsystem failures. Examples are the reliance of the building air cooling units (ACUs) on service water and electrical power supplies which may in turn have contributed to a core damage state, that of the hydrogen igniters on Class III and II power, the failure of the vacuum building pathway to the FAD system following loss of Class IV power or low pressure service water due to the resulting inoperability of the vacuum pumps, etc.

For instance, the most likely cause of EPRC1 is the loss, coincident with a LOCA, of the even power distribution systems in conjunction with a dormant diode failure in an odd 48 V dc supply, and a pre-existing containment impairment. Inadequate HPECI results due to failure to generate the LOCA conditioning signal to open sufficient shutdown cooling system isolation valves as a result of the loss of the 48 V dc supply. Moderator system failure occurs due to inability to backwash service water travelling screens and trip condenser cooling water (CCW) pumps due to the loss of the even power supplies. The reactor building ACUs fail as well due to the loss of the power supplies.

Dominant contributors to EPRC2 arise from an unrecovered loss of low pressure service water, which leads to loss of main and auxiliary feedwater, as well as shutdown cooling. The coincident failure of the emergency boiler water system leads to core damage. The

Table 5:
Frequency Results for EPRCs

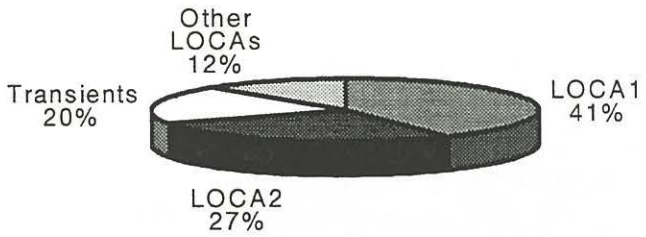
EPRC	Description	Mean Frequency (per reactor.yr)
EPRC1	Early core disassembly with pre-existing opening	4×10^{-10}
EPRC2	Slow core disassembly with pre-existing opening	6×10^{-9}
EPRC3	Late consequential failure due to hydrogen explosion	9×10^{-8}
EPRC4	Intermediate release in STP1	2×10^{-8}
EPRC5	Containment bypass	2×10^{-8}
EPRC6	Reactivity excursion and early consequential containment cracking	3×10^{-7}
EPRC7	Late release through filtered air discharge	1.3×10^{-4}

ACUs are unable to condense the steam in the reactor building as a result of the loss of low pressure service water and the resulting inability, for example due to flooding, to valve in an alternate water supply from inter-unit ties. This provides the pressurization to drive fission products out of containment through an unrecovered pre-existing opening in any of the six building airlocks.

In EPRC3, a dependency of the emergency coolant recovery/ moderator heat sink and the hydrogen ignition system on an odd 4kv Class III power bus features in the dominant event sequences. The unrecovered loss of this bus leads to insufficient moderator flow, and, hence, loss of the emergency coolant recovery (ECR) and moderator heat sink functions, and, severe core damage. It further leads to failure of the fans associated with the air cooling units in the east fuelling machine vault, thus preventing adequate mixing of the atmosphere in this FM vault, and, failure of controlled ignition of combustible gases produced following the severe core damage event. However, the likelihood of operator recovery to prevent containment failure is high as an alternative power supply to the ACUs can be provided.

A key event sequence finding its way into EPRC3 is the loss of all electrical power due to the occurrence of a large steam line break in the powerhouse and inability to mitigate its effects by means of engineered features, such as the powerhouse venting system, or the Class I and II electrical room ventilation system. Failure of all of a unit's power supplies, Class I to IV, results in total loss of core cooling, and eventual core damage, as well as failure of the unit's hydrogen igniters. Only the FAD system remains functional since it is

Figure 5:
Contributors to Individual Delayed Fatality Risk by Initiating Event Type



powered from Pickering NGS B supplies. However, the FAD system can only delay but not prevent the formation of detonable mixtures in the reactor building given an initially intact containment. Thus, unless local burns can successfully burn off the combustible gases produced as a result of the interaction of the molten core with the concrete basemat of the reactor building, the failure of the hydrogen igniters may lead to a late containment failure.

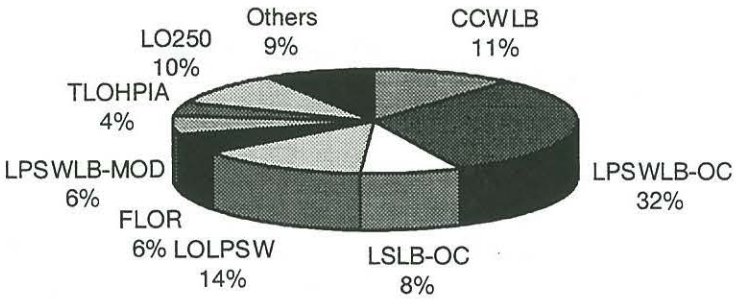
EPRC4 contains those sequences in which the core is damaged early in the accident, and a release occurs via a large pre-existing containment impairment before the FAD system can be placed in service. The delay in crediting the FAD system is postulated to be caused by water-plugging of the HEPA filters due to the presence of steam in the containment atmosphere. The major cause of core damage is the unrecovered draining of the moderator inventory after a LOCA2 or bigger break.

EPRC5 is the set of all sequences in which HT coolant blows back into the HPECI system, leading to the latter's failure as well as a loss of containment. If additionally, the moderator heat sink also fails, for example, due to its also being drained to the break through the ECR injection valves, both an in-plant as well as an ex-plant release occurs. Similarly, steam generator tube breaks with failure of HPECI and the moderator heat sink, coupled with inability to close the steam reject valves, also lead to an off-site release of the kind represented by EPRC5. The fact that, once core disassembly begins, the primary release pathway is into the subatmospheric containment, contributes to the relatively small off-site release associated with the category.

The set of events in which the reactor fails to be shut down after a reactivity insertion, with the release occurring either due to a small opening in the containment envelope or as a consequence of failure to shut down, contribute to EPRC6. Finally, those core damage events in which all containment mitigating systems operate but a release of noble gases occurs over the long-term via the FAD system were placed in EPRC7. Dominant contributors to EPRC7, as is obvious, are the same as that to fuel damage category FDC2.

An illustration of the relative importance of initiating events to one of the public health risk measures defined in Section 4 is given in Figures 5 and 6.

Figure 6:
Breakdown of Transient Initiator Contributors to Individual Delayed Fatality Risk



Initiating events additional to those appearing in Figures 2 and 3 are; a fast loss of reactor power regulation (FLOR), large steam line break outside containment (LSLB-OC), LPSW line break in the supply to the moderator system (LPSW-MOD) and total loss of high pressure instrument air (LOHPIA).

5 SUMMARY OF PARA RESULTS AND CONCLUSIONS

5.1 Summary of Risk Results from the PARA

A summary of the major numerical results of the study is given in Table 6. Maximum individual risk is that calculated for a hypothetical individual at the site boundary, dose exposure risk being converted to latent fatality risk at the rate of 5% per Sievert. Ontario Hydro's three trial risk-based safety goals are shown for comparison purposes.

The results show that all three current safety goals are met. The very low offsite risks, which arise in part from the benefits of a multi-unit, shared containment station design, is contrasted with the high onsite property damage risk, which arises due to the same cause.

A quantitative uncertainty analysis was performed for some selected outputs based on probability distribution functions provided for all basic event failure probability data and consequence analysis significant to the risk calculation. The relatively small ratios between the 95th percentile and the mean values is a reflection of the presence of many independent variables in the risk equation

5.2 Discussion of Results

The PARA has calculated generally very low frequencies for significant releases of radioactivity off-site. These low frequencies are not merely artifacts of the risk assessment methodology but are the result of specific aspects of the station design;

(a) the pressure tube design of CANDU reactors;
(b) the multi-unit, negative-pressure containment system; and,
(c) continuous on-power fuelling.

The most likely sequences leading to core disassembly involve failures of primary and emergency heat removal systems, leading to moderator draining, boil-off and progressive uncovering of fuel channels. Under these conditions, CANDU fuel channels fail relatively early, analogous to a pressure *fuse*. If primary circuit depressurization has not already occurred due to an initiating LOCA, failure of the first fuel channel will cause rapid HT system depressurization initially into the calandria and subsequently, via the calandria rupture discs, into containment. Any further core degradation will occur at low HT system pressure, reducing the potential for energetic release of core materials and fission products, and limiting the potential for challenging containment integrity.

Rapid and near-simultaneous failure of multiple fuel channels can be postulated to accompany a fast, uncontrolled reactivity transient. At the extreme, this can lead to structural failure of the calandria and expulsion of the moderator. However, the dispersal of fuel that results from the initial violent pressure surge creates a large cooling surface area that limits the rate of fuel heat-up and accompanying early fission product release to containment and, as a result, to the environment.
For both types of sequence discussed above, any long term accident progression takes

Table 6:
PARA Integral Results (Point Values) for Accident Risk

MEASURE	MEAN	95% CONFIDENCE	Comments
Maximum Individual Early Fatality Risk	2.5×10^{-8} per station-yr	-	Safety Goal = 1×10^{-6} per station-yr
Maximum Individual Latent Fatality Risk	4.4×10^{-7} per station-yr	1.2×10^{-6}	Safety Goal = 1×10^{-5} per station-yr
Societal Latent Fatality Risk	1.3×10^{-3} per station-yr	-	
Large Release Frequency	1.2×10^{-7} per reactor-yr	3.6×10^{-7}	Safety Goal = 1×10^{-6} per reactor-yr
Severe Core Damage Frequency	1.3×10^{-4} per reactor-yr	3.4×10^{-4}	
Onsite Property Damage Risk	$60 Million per station-yr	-	
Offsite Property Damage Risk	$1000 per station-yr	-	

place inside a containment maintained at, or more likely slightly below, atmospheric pressure. The response to internal pressurization of the reinforced concrete structure of the buildings that constitute the containment envelope tends to reduce the likelihood of catastrophic containment failure. The expected behaviour is local yielding of reinforcement and cracking of the envelope, leading to pressure relief and followed by reclosure. No credible causes of catastrophic failure were identified.

For those sequences involving a failure of the HT system leading to containment bypass, the driving force for release out of the PHT system impairment bypassing containment is removed once core disassembly begins. More likely, the flow direction reverts into the subatmospheric containment via the calandria relief ducts. Because of this, severe accident sequences initiated by an event causing a containment bypass pathway, such as steam generator tube failures or the spurious opening of emergency coolant injection valves (called *blowback* in the PARA but also referred to elsewhere as the *V sequence*), are benign in terms of off-site consequences compared to the equivalent sequences in designs which use a reactor pressure vessel.

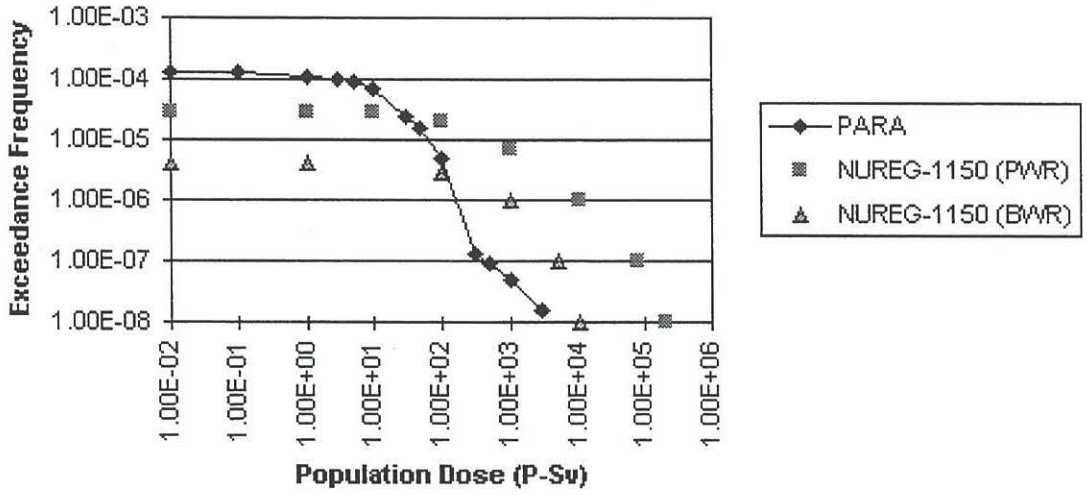
In sequences where failure of containment systems is postulated to lead to gradual pressurization of the accident unit, containment envelope failure is precluded in the near term because interconnection between the eight Pickering units will occur via the rupture/relief panel systems and the pressure relief duct. This greatly increases the effective volume of containment and the availability of heat removal. Only in the event of operator inaction for many days could pressurization sufficient to challenge containment envelope integrity be envisaged. The many opportunities for accident recovery that would be available over such a timescale effectively eliminate slow pressurization as a cause of containment failure.

Finally, because on-power fuelling reduces the average irradiation time of the fuel compared to that of light water reactors (LWRs), the core inventories of long-lived radioisotopes, which play an important part in the long-term consequences of large releases of radioactivity, are three to five times lower than their LWR counterparts per unit of thermal power produced. In addition, the electrical power output rating of the Pickering NGS A reactors at a nominal 540 MW is lower than that of more recent reactor designs (typically 800-1000 MW). As a result, the overall equilibrium core inventory of fission products is correspondingly lower. The outcome is that the Pickering NGS A reactors contain significantly less potential for off-site contamination by long-lived radioactivity.

Figure 7 shows the combined population dose CCDF from the PARA, along with equivalent results from for two US plants [7] for comparison purposes. The results exhibit characteristics which are typical of the CANDU reactor in a negative-pressure containment; a very low risk contribution from the high consequence end of the spectrum and a relatively high contribution from the low-consequence end. This reflects the PARA finding that there are very few mechanisms that can credibly cause catastrophic containment failure leading to a large release, but the need to discharge containment

atmosphere via the filtered air discharge system (in order to maintain containment at negative pressure) always results in some, albeit small, release for any accident.

Figure 7:
Comparison of PARA and NUREG-1150 Risk Profiles



5.3 Study Conclusions

The principal conclusions of the study were:

1) On the basis of comparison with safety goals, the risk to the health and welfare of the population living or working in the vicinity of the Pickering Nuclear Generating Station is significantly lower than other risks to which they are normally exposed.
2) The likelihood of an accident which could cause severe damage to the reactor core is similar to that for other contemporary reactor designs but higher than that for more recent CANDU reactors such as Darlington NGS. This is largely due to a lack of independence between the emergency coolant injection system and the moderator system. Despite the presence of only one fast-acting shutdown system, accident sequences resulting in rapid positive reactivity insertion do not appear to be significant to risk.
3) The likelihood of the occurrence of a catastrophic accident which could cause acute radiation effects beyond the site boundary is sufficiently small to be considered negligible for all practical purposes. Features unique to the CANDU pressure-tube design and the multi-unit, negative-pressure containment contribute to a very low overall risk to public health and welfare.
4) External economic risks from the accidental release of airborne radioactivity off-site are correspondingly low. The internal economic risk to Ontario Hydro from an

accident involving fuel damage is comparable to that from its other stations, with the dominant contribution arising from the relatively more likely, low consequence events. Both the low offsite risks and the relatively high onsite risk result from the multi-unit containment design.

The PARA was produced as part of an ongoing risk assessment program at Ontario Hydro Nuclear. Current plans include the Bruce B Risk Assessment (BBRA), the Bruce A Risk Assessment and an updated Darlington Risk Assessment (DARA).

REFERENCES

1. "The Pickering A Risk Assessment", Ontario Hydro, November 1995.
2. The US Nuclear Regulatory Commission, "Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance, (Draft Report)", Washington D.C., NUREG -1560, October 1996.
3. "The Darlington Probabilistic Safety Evaluation", Ontario Hydro, December 1987.
4. Wahba N.N., Y.T. Kim, P.M.Petherick and S.G. Lie, "Timing of Core Damage States Following Severe Accidents for the CANDU Reactor Design", Paper presented at the 17th Annual CNS Conference, Fredericton, N.B., June 1996.
5. Wahba N.N., Y.T. Kim, "Consequence Analysis of Core Damage States Following Severe Accidents for the CANDU Reactor Design", Paper presented at the 18th Annual CNS Conference, Toronto, ON, June 1997.
6. Chanin, D.I. et al, "MELCOR Accident Consequence Code System (MACCS)", User's Guide, NUREG/CR-4691, SAND86-1562, February 1990.
7. The US Nuclear Regulatory Commission, "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants", Washington D.C., NUREG-1150, Volume 1, December 1990.