MONITORING THE RISK OF LOSS OF HEATS SINK DURING PLANT SHUTDOWNS AT BRUCE GENERATING STATION "A".

K. S. KRISHNAN, P. ENG.
SR. TECHNICAL ENGINEER
ONTARIO HYDRO
BRUCE GEN. STN. "A"
P. O BOX. 3000
TIVERTON, ON, N0G 2T0

F. MANCUSO, P. ENG.
NUCLEAR DESIGN ENGINEER-SPECIALIST
ONTARIO HYDRO
700 UNIVERSITY AVENUE
TORONTO, ON, M5G 1X6

D. VECCHIARELLI, P.ENG.
NUCLEAR DESIGN ENGINEER-SPECIALIST
ONTARIO HYDRO
700 UNIVERSITY AVENUE
TORONTO, ON, M5G 1X6

ABSTRACT

A relatively simple Loss Of Shutdown Heat Sink Fault Tree model has been developed and used during unit outages at Bruce Nuclear Generating Station "A" to assess, from a risk and reliability perspective, alternative heat sink strategies and to aid in decisions on allowable outage configurations. The model is adjusted to reflect the various unit configurations planned during a specific outage, and identifies events and event combinations leading to loss of fuel cooling. The calculated failure frequencies are compared to the limits consistent with corporate and international public safety goals. The Importance Measures generated by the interrogation of the Fault Tree model for each outage configuration are also used to reschedule configurations with high Fuel Damage Frequency later into the outage and to control the configurations with relatively high probability of Fuel Damage to short intervals at the most appropriate time into the outage.

1.0 Introduction

A basic operating philosophy for CANDU stations has always been to provide a Primary Heat Sink that consists of a means of transporting heat from the fuel, a means of removing the heat from the heat transport medium to a heat sink, and the availability of an alternative method of cooling the core. Heat sinks are selected for outage units on the basis of the systems capacity to dissipate the decay heat. Alternate heat sinks are selected on the basis of using systems that are independent of those required by the primary heat sink which is normally in service. These principles have been embedded in the Operating Policy and Principles of the stations since the earliest days. As international and domestic experience grew, it was recognized that the loss of the heat sinks during outages might be a significant contributor to the risk of core damage.

Bruce A is experiencing an increase in planned and unplanned outages as a result of rehabilitation activities and plant aging. The complexity and longer duration of those outages imposes an increased demand on the specification and monitoring of systems which impact on fuel cooling. The specification of heat sinks at Bruce A must also take into account the potential for heat sinks to be affected by accidents on other at power units which share a common powerhouse.

A team approach was used to achieve safe and successful outages. During a preoutage multidisciplinary team meeting (called Task Analysis meeting) components and systems which have a primary, alternate and emergency heat sink significance are identified for each outage activity. Before and during the outage, heat sink availability is reviewed with outage supervisors and planners to ensure that the heat sink requirements are met. When unforeseen changes in outage configuration arise, task analysis meetings are initiated and the appropriate heat sink strategies confirmed.

The tools used for the monitoring of the Outage Heat Sinks are a Loss of Shutdown Heat Sink Fault Tree[1], a PC based Reliability and Risk Model Interrogation Code (RRIMIC)[2] model, RISKPLOT[3] graphs and the appropriate targets and limits on the Fuel Damage Probability values. It was felt that the development of a

logic model representing means by which a loss of shutdown heat sink could occur at Bruce A would be valuable in ensuring heat sink reliability. Preliminary work at developing such a model had already been carried out for Bruce generating station "B"[4]. This Loss of Heat Sink model was adapted to Bruce A and extended to include not only events representing random failures of systems and equipment critical to the heat sink function (including electrical, water and air service systems), but also events representing intentional system/equipment maintenance outages. The following sections of the paper deal with the theory behind the development of these tools and the methods adopted to monitor the risk of the Bruce A units during outages.

2.0 Loss of Shutdown Heat Sink Fault Tree

2.1 Summary

In the fault tree model developed for Bruce A, the four distinct operating states that can be entered during a generic outage are analyzed separately. The analyzed states are: heat transport system closed, heat transport system open at the boiler plenum manways, heat transport system open at a pump bowl and heat transport system open at main circulating pump seal. For each of these states, a reference case with no maintenance outages is assessed. The reference cases are then adjusted to reflect the various specific unit outage configurations. These assessments are conducted using the PC-based fault tree model interrogation code RRIMIC (Reliability and Risk Model Interrogation Code).

2.2 Alternate Heat Sink Strategy

At Bruce A, the normal heat sink during a long-term outage is the Maintenance Cooling System (MCS). Following a failure of the MCS, the alternative means of decay heat removal which could be used during a unit outage depend on the availability of the systems that provide or support reactor heat sink functions for the specific operating state of the heat transport (HT) system.

Irrespective of the initial state of the HT system, the preferred alternative heat sinks are the steam generators or the shutdown cooling (SDC) system if available. In order to establish either of these heat sinks, the operator is required to

a) Close the HT system if open,

b) Re-fill and re-pressurize the HT system,

c) Provide a secondary side heat sink by supplying water to the steam generators and providing a means of relieving steam to the atmosphere and ensuring circulation of HT coolant through the reactor core.

OR

Place in service the SDC system, if available, which requires pressurizing the secondary side of the preheaters with the auxiliary boiler feed water pump and establishing forced circulation with the HT system pumps.

Since the unit's D_2O storage tank has insufficient inventory to re-fill the HT system when it is initially in the low level drained state, extra supplies of D_2O need to be obtained from the non-accident units and/or the D_2O supply system.

Normally, water to the steam generators is supplied from the de-aerator storage tank by means of the auxiliary boiler feed pumps. If the feedwater system is not available, the inter-unit feedwater tie (IUFWT), which connects the feedwater systems of all reactor units, can be used as an alternative source of water. If the IUFWT as well is not available, the Emergency Boiler Cooling system (EBC), drawing water from the lake, is able to provide a supply of water to the steam generators. Steam discharge is effected by means of the Boiler Safety Relief Valves (BSRVs).

Following successful closure of the HT opening, filling and pressurizing of the HT system, the main PHT circulating pumps are started. Thermosyphoning can also be relied on to transfer reactor heat to the steam generators if the PHT pumps cannot be kept running. However, at least one main PHT pump is required to operate briefly to establish a thermosyphoning flow from the stagnant state that results on loss of the maintenance cooling pumps.

In the event the HTS system opening cannot be closed within 30 minutes of MCS failure, fuel cooling can still be provided by injecting water to the reactor headers from the EBC or Emergency Coolant Injection (ECI) systems. The method of heat removal from the core depends on the location of the HT system opening. The injected water supply, after exiting from the HT opening, accumulates in the reactor building sump. In the longer term, the emergency coolant recovery system would be used to provide a means of core cooling, except if the pump is open, in which case the opening is outside containment and MCS heat sink must be restored in the long term.

If the HT system is successfully closed but not filled due to failure of feed and bleed, ECI and EBC systems, Intermittent Buoyancy Induced Flow (IBIF) to the reactor headers and steam rejection through the boiler SRVs is a credible heat sink provided EBC water supply to both steam drums is available.

If the opening is in the main circulating pump seal and cannot be closed, IBIF to the reactor headers and steam rejection through the boiler SRVs is still a credible heat sink provided that a cold EBC water supply to both steam drums and a source of HT system coolant makeup is available.

2.3 Fault Tree Top Events

The following top events are defined for the purpose of the fault tree analysis of the four basic shutdown configurations:

a) ***"Loss of fuel cooling during reactor shutdown when MCS in use and HTS closed".***

b) ***"Loss of fuel cooling during reactor shutdown when MCS in use and HTS pump bowl open".***

c) ***"Loss of fuel cooling during reactor shutdown when MCS in use and HTS pump seal open".***

d) ***"Loss of fuel cooling during reactor shutdown when MCS in use and boiler man-ways open".***

2.4 Fault Tree Analysis

2.4.1 Equipment Status During Outage

During the outage, some systems and components may be either unavailable due to maintenance or isolated due to work protection. Once the maintenance work is completed, repaired equipment are tested and returned to service. To capture the configuration changes that occur during the outage, failures of systems and equipment that could affect the shutdown heat sink capability, if taken out of service, are included in the model with the expected failure probabilities. To determine the changes to fuel cooling frequency caused by taking the relevant equipment out of service, the failure probability of these events is set to 1 in the RRMIC models.

2.4.2 Design, Operational, and Modelling Assumptions

The model development is based on the following key design, operational and modelling assumptions.

2.4.2.1 Alternate Heat Sinks

i) The preferred alternate heat sink to maintenance cooling system is the steam generator heat sink. If the heat transport system is open, measures will be taken to close it in order to use this heat sink. The

operators are also expected to perform parallel activities to place in service the SDC system, if available.

Steam generators and SDC heat sinks require HT system filling, if initially open, forced coolant circulation, feedwater supply to at least one steam drum and steam rejection via boiler SRVs.

ii) If the HT system is successfully closed but cannot be filled due to failure of feed and bleed, ECI and EBC systems, cold EBC water will be supplied to both steam drums and steam rejected through the boiler SRVs. IBIF to the reactor headers with condensation in the boiler tubes will ensure fuel cooling.

iii) If the HT system is successfully closed and filled but forced circulation cannot commence due to failure to bump at least one HT system PHT pump, cold EBC water will be supplied to both steam drums and steam rejected through the boiler SRVs. Coolant circulation will be provided by the IBIF phenomenon as steam vented from the core would be condensed by the subcooled liquid outside the core.

iv) If the heat transport system cannot be closed and the opening is in the boiler manways, cooling water will be supplied to the reactor core from ECI or EBC and discharged from the opening.

v) If the opening is in the pump bowl and cannot be closed, one core pass will not receive an injection flow regardless of the location of the opening and the injection path. This core pass can be cooled by IBIF to reactor headers as long as the HT headers can be filled.

vi) If the opening is in the pump seal and cannot be closed, coolant discharge through pump seal opening cannot by itself provide sufficient heat removal. Additional cooling will be provided by IBIF to the reactor headers and steam rejection through the boiler SRVs. For this fuel cooling mechanism, cold EBC water supply to both steam drums and a source of coolant makeup will be required.

2.4.2.2 **Coolant Circulation**

i) At least one main PHT pump is required to briefly run to initiate a thermosyphoning flow through the reactor core in order to transport decay heat to the steam generators.

ii) At least one main PHT pump is required to start and run to maintain continuous forced circulation.

iii) If SDC is used, forced circulation is required to transfer reactor heat to the preheaters.

iv) Following loss of MCS flow with HT system closed and full, IBIF coolant circulation will occur if both steam drums are supplied with cold EBC water even if no PHT system pump is available to start coolant circulation.

2.4.2.3 **HT Pressure Relief Path**

i) If the HT system is initially closed, pressure relief path is required to protect the HT system against excessive coolant swell that occurs while establishing the boiler SRV heat sink.

ii) Depending on the specific maintenance work, the HT system pressure relief path is to be defined.

iii) Failure to provide HT system pressure protection (by means of a single liquid relief valve) is conservatively assumed to contribute to the loss of shutdown heat sink..

2.4.2.4 Steam Generator Feed Water Supply

i) Feed water flow to the secondary side of boilers can be provided by means of the IUFWT or EBC systems. Only the latter can be credited if coolant circulation is by means of thermosyphoning or, if fuel cooling is achieved by IBIF to reactor headers and condensation in the boiler tubes as, in these cases a cold water supply to the steam generators is required.

For thermosyphoning, EBC water supply to one steam drum is deemed sufficient. For IBIF, EBC water supply to both steam drums is required.

At least one steam generator in each of the two steam drums is kept full of water prior to the loss of MCS cooling.

2.4.2.5 Boiler Steam Relief

i) Only boiler safety relief valves are credited for boiler steam rejection.

2.4.2.6 Long Term Heat Removal

i) If the HTS is open to containment and cannot be closed, emergency coolant recovery must be established in the long term on a loss of MCS. Electrical power is provided to the EBC by the harsh environmentally Qualified Power Supply (QPS). A jumper connection between the EBC system and MCS system allows the makeup flow to be established to the HTS from outside the powerhouse within 30 minutes of a Main Steam Line Break (MSLB) event. If the HTS is open outside containment, and cannot be reclosed, restoration of the MCS provides the long-term heat sink. To allow for an extended loss of Class III and Class IV power, a portable diesel generator is located outside the powerhouse to provide electrical power via jumper cables to one MCS pump motor and one LPSW pump motor. This will ensure restoration of MCS circulation, Heat Exchanger flow and MCS pump glands flow within 12 hours following a MSLB event (See item ii of Subsection 2.4.2.7 below).

2.4.2.7 Steam Line Break Effects on Outage Reactor Unit.

Plant response following a steam line break in one of the operating units is as follows:

i) Class I to IV electrical power systems are assumed to fail in all units in the station, and only the qualified power system is credited to be operable.

ii) MCS heat sink is lost due to power failure. After the powerhouse becomes accessible, it is, however, expected that the operators will be able to restore MCS heat sink by connecting one MCS pump and one LPSW pump to a diesel generator.

iii) Forced circulation by MCS fails and natural thermosyphoning circulation of reactor coolant cannot be initiated as HT pumps may not be bumped. If the HT system is closed and full, IBIF circulation of the HT system coolant will occur.

iv) A pump bowl opening cannot be closed and a boiler manway has only a small chance (assumed to be 10%) of being successfully closed.

v) ECI water supply to HT system fails due to loss of power and failure to manually open ECI test valves 3433-MV101 and MV102 because of the harsh environment. Coolant makeup is from EBC system via direct jumper connection to MCS.

vi) The HT feed/bleed system is unavailable to pressurize the HT system due to loss of power.

2.4.3 Failure Criteria

A total loss of fuel cooling may occur during shutdown if the operators fail to establish an alternate heat sink following failure of the MCS heat sink. The failure criteria of the main and alternate heat sinks are briefly described in the following subsections.

2.4.3.1 MCS Heat Sink Failure Criteria

The maintenance cooling system fails to cool fuel if :

- Both MCS pumps fail to circulate cooland due to either mechanical electrical problems or gland failures.

OR

- Both heat exchangers are unable to reject heat due to system failures such as temperature controller problems, loss of LPSW etc.

2.4.3.2 Alternate Heat Sink Failure Criteria

In addition to operator's failure to detect a loss of MCS, failure of the alternate heat sinks depend on the existing operating conditions. The alternate heat sinks fail if any of the following failures occur:

a) the steam generators and SDC system (if available) fail to remove decay heat given the HT system is closed if initially open, or,

b) an injection flow fails to be provided to the core from the ECI or EBC systems if the HT system is initially open at the boiler manway or pump bowl and is not closed, or,

c) an injection flow fails to be provided through the core from the ECI or EBC systems or cold EBC water supply to both steam drums fails to be provided if the HT system is initially open at the pump seals and not closed, or,

d) cold EBC water supply to both steam drums fails to be provided if the HT system is closed if initially open, or,

e) HT system pressure relief fails due to inability of the single available liquid relief valve to accommodate coolant swell when placing the steam generator heat sink in service.

2.5 Equipment Failures

Changes of heat sink failure frequency caused by taking a system out of service for maintenance can be monitored by setting the probability of a system failure event to 1 in the fault tree model. The model then assumes that the system is not available to perform or support a heat sink function.

Similarly, failure of equipment that support heat sink functions, such as electrical buses which may be isolated for maintenance during the outage, are also included in this fault tree model.

2.6 Human Errors

Most of the human errors postulated in the fault tree are the post initiating event errors, such as failure to valve in the alternate heat sink, or failure to start the EBC pump, etc. Preliminary values of these were obtained from the Ontario Hydro's risk assessment fault tree guide[5]. The analyst has to make judgments as to the complexity of the task at hand, the quality of the indications provided, and the time available.

2.7 Fault Tree Solution

The Loss of Shutdown Heat Sink fault tree supported by the primary event data is solved (i.e., its minimal cutsets obtained for four top events, HSNK-HTS-CLOSED, HSNK-PBWL-OPEN, HSNK-PSEAL-OPEN, HSNK-BOILER-OPEN) by means of the SETS code. The minimal cutsets obtained for each of the four top events identify the contributors to failure of core cooling for each of the four basic HT shutdown states, viz., closed, open at the boiler plenum manways, open at the pump bowls and open at pump seals. The minimal cutsets, which are obtained assuming that all systems and equipment that support heat sink functions are available, are used to produce the four reference cases of the RRIMIC models.

During the progression of the shutdown activities, system configuration changes occur as equipment is repaired, tested and returned to service. Each shutdown configuration is simulated on a PC work station by changing the relevant failure probabilities used in the reference cases of the RRIMIC models to reflect the actual state of the equipment. The models are then interrogated to determine the predicted core cooling failure frequency (FDF) for each specific shutdown configuration.

2.8 Results

The Fuel Damage Frequencies for various outage configuration of shutdown units are included in the paper. The procedure to determine the relative risk levels is summarized as follows:

- Determine the Outage Logic from Outage Planning.
- Determine the equipment states.
- Determine the time from shutdown and duration of the occurrence of these outage states from the Level 1 Unit Outage Plans.
- Run the RRIMIC model for Loss of Shutdown Heat sink for each of the outage configuration.
- Reconfigure the outage logic if necessary to reduce the risk of loss of heat sink to an acceptable level.

3.0 RISKPLOT

A computer application called RISKPLOT is used at Bruce A to assess the risk of loss of heat sink during plant shutdown.

The function of the RISKPLOT is to generate the following two risk plots:

- The fuel damage frequency (FDF) versus shutdown time.
- The integrated fuel damage probability (FDP) versus shutdown time.

The FDFs (due to loss of heat sink for various phases of shutdown) calculated by RRIMIC, using the Shutdown Loss of Heat Sink risk model, are entered into RISKPLOT to generate the above mentioned graphs. The graphs produced by RISKPLOT are used as guidelines for scheduling the various shutdown phases to minimize the risk of loss of heat sink during plant shutdowns.

3.1 Risk-based Control of Plant Configurations

The risk from a nuclear plant will change (increase or decrease) as the plant configuration varies, whether the plant is operating or in shutdown state. Various plant configurations occur, for example, when different components are taken out of service for maintenance.

The risk of a plant shutdown configuration includes the following two factors:

F_i = the FDF caused by a plant configuration i in the shutdown state, and
d_i = the duration of the shutdown plant configuration i.

The product of F_i and d_i yields the fuel damage probability (FDP) for a plant shutdown configuration i.

The integrated FDP contribution (RT) caused by all the plant configurations during the shutdown period T can be written as:

$$R_T = \sum_{i=1}^{n} [F_i \times d_i]$$

where, n is the number of different plant configurations during the shutdown period T.
R_T is the probability of a loss of heat sink over the shutdown period T.

There are two different basic strategies for controlling plant risk during its shutdown period T:

1. control the FDF level, and /or
2. control the duration of the events with high FDF level.

The only way FDF peaks can be controlled is by mitigating critical plant configurations which cause large FDF peaks. This may be achieved by appropriate scheduling of tests and maintenance of critical components. The importance measures generated from the Loss of Shutdown Heat Sink risk model are used to provide direction in this regard.

R_T can be controlled by minimizing FDFs and/or duration of shutdown plant configuration and by appropriately scheduling high FDF configurations later in the outage.

3.2 Shutdown Risk Control Limits

In order to use the FDF and R_T as measures for controlling the Loss of Shutdown Heat Sink risk, an FDF limit must be first established. The applied FDF Limit is 5×10^{-3} / unit-year, which is an order of magnitude above the derived target for normal operation. This target can be derived from the Ontario Hydro Risk-based Safety Goals[6]. Discussion on the FDF targets and limits is included in Section 4 of this paper.

3.3 FDF and FDP Graphs

The FDFs for the shutdown configurations are plotted against the shutdown time to show graphically the impact of the risk of loss of heat sink during shutdown. The FDF Limit and Target are also plotted on the same graph as guideline.

A FDP graph can be constructed from the FDF graph by plotting the integrated products of FDF and time duration for the shutdown configurations versus the shutdown time.
against risk target, risk limits, and estimated risk of normal unit operation to see that the risk is manageable and acceptable throughout the outage.

4.0 Criteria for managing Shutdown Accident Risk

The proper management of risk[7] during a planned outage can be assisted by the availability of appropriate risk measures and standards. Risk criteria are proposed as decision aids in the management of shutdown heat sink strategies. The first risk management ceitrion derived is based on the Ontario Hydro safety goal for individual delayed fatality, as this safety goal is expected to be limiting for accidents which may occur during planned shutdowns.

- *Fuel Damage Frequency Target* 5×10^{-4} /unit-year, or 2×10^{-3} /station-year

This frequency target is applicable soon after (say, > 3 hours) reactor shutdown, at any time thereafter and for any plant configuration, including an open heat transport system and/or containment bypass. The target is, therefore, highly conservative for most anticipated shutdown configurations.

A second set of risk management criteria comprises two allowable Fuel Damage Frequency Limits (based on state of containment) as a function of decay time for a given shutsown heat sink stragegy. As decay time increases, the frequency limits increase to maintain a constant risk with time. These frequency limits provide a more realistic, variable risk target that reflects the time dependence of accident consequences with increasing time and with the planned system configurations as the shutdown progresses.

4.1 Derivation of the Target and Limit values

4.1.1 General Assumptions

Several shutdown configurations may be employed during the course of a shutdown as equipment is repaired, tested, and returned to service. Thus, for each shutdown configuration there is associated accident frequency estimate referred to as a *fuel damage frequency (FDF)*. By combining the consequences (e.g., radiological or financial) associated with each FDF one can derive the risk for the shutdown period.

The consequence assessment is based on some simplifying assumptions as outlined below:

(a) The reactor unit is shutdown for planned maintenance.

(b) Two states of the heat transport system (HTS) are considered:

1. Assumed to be open to containment (e.g., via the boiler manways).

2. Assumed to be open such that containment is bypassed (e.g., via the pump bowl).

(c) Normal means of containment pressure control may not be available (e.g., vault coolers may not be available due to selected electrical bus outages during the shutdown). To minimize the number of cases, any impaired containment configuration was conservatively assumed equivalent to containment bypass.

A loss of heat sink under shutdown conditions can, in principle, have a wide range of potential consequences. From the point of view of fission product decay, the length of time the reactor unit has been shutdown prior to a loss of cooling to the fuel can strongly influence the potential dose consequences to the public.

4.1.2 Consequence Modelling

4.1.2.1 Methodology

The tool used to calculate the time dependence of public or off-site doses is the Bruce NGS Emergency Response Projection program (BERP)[8]. BERP makes dose projections for the area surrounding Bruce A resulting from airborne releases following a nuclear accident. This program is intended for real-time use following an accident, but can be used to examine the time-dependence of consequences for a given accident.

4.1.2.2 Public Dose

Two release scenarios based on the state of the HTS are considered in the analysis of the public consequences. These are listed below and described in the proceeding subsections.

Scenario 1 - Containment Intact

Scenario 2 - Containment Bypass

4.1.2.2.1 Scenario 1 - Containment Intact (HTS Open to Containment)

In this scenario, the containment system is assumed fully functional and the unit is isolated. The HTS is assumed open inside containment. Thus, any releases resulting from a loss of cooling to the fuel will occur within containment. Releases outside of containment are via the Emergency Filtered Air Discharge System (EFADS).

This scenario is also used to bound shutdown configurations in which the HTS is initially closed.

An equation (using the BERP program) for the public dose as a function of decay time was derived for the containment intact scenario as follows:

$$dose_{ci}(t) = e^{-0.0052t-0.07} \times 3x10^{-3}\ Sv$$

where, $dose_{ci}(t)$ = Public dose at time of accident after shutdown, given a containment is intact.

t = time of accident after shutdown, in hours, taken at the beginning of the shutdown configuration.

$3x10^{-3}\ Sv$ = Safety Report small LOCA*LOECI total whole body dose, i.e., 3 x 10^{-2} Sv (individual) reduced by a factor of 10 to account for the effect of radioactive decay in the source trem due to the fact that shutdown tasks would not have commenced until some time after the unit is shutdown.

4.1.2.2.2 Scenario 2 - Containment Bypass (HTS Open at Containment Boundary)

This scenario represents the shutdown configuration in which the containment system is bypassed (e.g., via the HTS pump bowl). Thus, some fraction of the releases resulting from a loss of cooling to the fuel is postulated to escape through the opening and bypass containment, thereby resulting in unfiltered releases.

A public dose equation was derived for Scenario 2 using the same basic procedure developed for Scenario 1. To account for the effect of containment bypass, the BERP program inputs were modified.

The equations for the public dose as a function of decay time derived for the containment bypass scenario are:

$$dose_{cb}(t) = e^{-0.0235t-0.0489} \times 0.1\ Sv\ ,\quad for\ 0 < t < 68.5\ hours$$

$$dose_{cb}(t) = e^{-0.0055t-0.8759} \times 0.1\ Sv\ ,\quad for\ t \geq 68.5\ hours$$

where, $dose_{cb}(t)$ = relative public dose at time of accident after shutdown, given a containment bypass exists

t = time of accident after shutdown, in hours, taken at the beginning of the shutdown configuration.

0.1 Sv. = Since no available Safety Analysis is applicable, a repersentative dose calculated by BERP beginning at time zero into shutdown (1 Sv) was reduced by one order of magnitude to account for the effect of radioactive decay in the source trem due to the fact that shutdown tasks would not have commenced until some time after the unit is shutdown.

5.0 FDF Target and Limit used for Planned Outages at Bruce "A"

The FDF target (a constant) for the planned outage period is derived from the Ontario Hydro public risk[4] goal for *individual delayed fatality* of 1.0×10^{-5} per station-year or 2.5×10^{-6} per unit-year. The proposed target is applicable soon after (say, > 3 hours) reactor shutdown.

Given the 5×10^{-2} probability of delayed fatality per Sv of radiation dose recommended by the International Commission on Radiological Protection (ICRP), and assuming the worst case public individual dose (i.e., 0.1 Sv for the containment bypass scenario in the initial stage of the shutdown t = 0), the FDF target is:

FDF Target = Ontario Hydro public risk goal for *individual delayed fatality* ÷ (probability of delayed fatality per Sv of dose × the worst case public individual dose)

$$\text{FDF Target} = 1 \times 10^{-5} \text{/station-year} \div (5 \times 10^{-2}\text{/Sv} \times 0.1 \text{ Sv})$$

$$= 2 \times 10^{-3} \text{ /station-year, or } \mathbf{5 \times 10^{-4} \text{ /unit-year}}.$$

This is consistent with the safety goal approach.

On the basis that the containment bypass scenario public dose was used in its derivation, the FDF target is expected to bound all shutdown configurations. Thus, for any shutdown configuration, at any time after about 3 hours, *if the FDF target is met, then the Ontario Hydro safety goal is assured to be met.*

For a shutdown configuration which exceeds the FDF target, it's FDF can be measured against one of two FDF limits, which are essentially allowable FDFs calculated taking into consideration the shutdown configuration (i.e., containment intact or containment bypassed/impaired) and the timing of the accident. Thus, each FDF limit is the maximum FDF for a given shutdown configuration such that the individual delayed fatality safety goal is not exceeded. The FDF limits are derived by dividing the delayed fatality safety goal by the product of public dose calculated at time t taken at the beginning of the shutdown configuration and the 5×10^{-2} probability of delayed fatality per Sv, viz.:

for containment intact,

$$FDF\ Limit_{ci}(t) = \frac{2.5x10^{-6} / unit - yr}{e^{-0.0052t-0.071} \times 3x10^{-3}\ Sv \times 5x10^{-2} / Sv}$$

for containment bypassed or impaired

$$FDF\ Limit_{cb}(t) = \frac{2.5x10^{-6} / unit - yr}{e^{-0.0235t-0.0489} \times 0.1\ Sv \times 5x10^{-2} / Sv}, \quad for\ 0 < t < 68.5\ hour$$

$$FDF\ Limit_{cb}(t) = \frac{2.5x10^{-6} / unit - yr}{e^{-0.0055t-0.8759} \times 0.1\ Sv \times 5x10^{-2} / Sv}, \quad for\ t \geq 68.5\ hours$$

FDF limit is the maximum FDF for a given shutdown configuration such that the individual delayed fatality safety goal is not exceeded.

- *Fuel Damage Frequency Limit used at Bruce A for the outages is* : 5×10^{-3} /unit-year or 2×10^{-2} /station-year, which is one order of magnitude greater than the target.

- *Fuel Damage Frequency Target value for a running or operating unit for comparison purposes is* 1.3×10^{-4} */unit-year*. This is based on the results of other risk assessments .

6.0 Conclusion

The fault tree model of Loss of Shutdown Heat Sink is now routinely used during the unit outages at Bruce A to confirm that the Loss of Shutdown Heat Sink risks are acceptably low, and as an input in decisions on allowable outage configurations. The Loss of Shutdown Heat Sink fault tree was used during the Unit 1 outage on 19th September 1995, Unit 2 outage on 9th October 1995 (this unit is on an extended outage awaiting retubing), Unit 3 outage from 4th November 1995 and the Unit 4 outage on 31st March 1995. Data on Unit 1 and Unit 3 with the graphs are included at the end of the paper.

The risk graphs and the importance measures gave guidance as to which systems failures contributed to the high FDFs, and the results of these risk assessments helped the Outage Management to be confident that the outage risk is manageable and acceptable through the outage. The calculate risk was compared against risk target, risk limits, and estimated risk of normal unit operation both prior to the outage planning and before any change in the planned configuration was undertaken during the outage.

Some of the high FDF configuration which were analysed include bus inspections in Unit 1, LPSW outage in Unit 3 where we took credit for supplying LPSW from Unit 4, QPS Breaker outage in Unit 4 and Class II bus replacements in Unit 3 and Unit 4.

7.0 REFERENCES

1. *Bruce NGS A - Fault Tree Analysis of Loss of Shutdown Heat Sink in Support of Unit 4* Outage *of April 1995.* (Draft) Report No. NK21-03611.6-955041-RO, April 1995.

2. *Reliability and Risk Model Interrogation Code (RRIMIC).* Technical Manual, Ontario Hydro Report No. 92207, Rev. 1, July 1993.

3. *Technical Manual for RISKPLOT - A Bruce NGS- A Outage Management Application Software.* March 1995.

4. *Fault Tree Analysis of Loss of Shutdown Heat Sink in Support of Unit 5 Outage of October 1994.*

5. *Risk Assessment Fault Tree Guide*, Ontario Hydro Report N-Rep-03611.2-0015, Rev. 0, February 1995.

6. *Risk-based Safety Goals for Ontario Hydro Nuclear Generating Stations.* Design and Development Report No. 89412, April 1990.

7. *Proposed Approach and Criteria for Managing Shutdown Accident Risk.* (Draft) Report No: N-03611.1- 95502-R0 , March 1995.

8. *Bruce NGS Emergency Response Projection Program - User Manual.* Revision 1.0, April 1992.

ACKNOWLEDGMENTS

The contributions of P.C.Chow and T.J. Ravishankar of Reliability Data and Support Unit and K.S. Dimnie of Consequences and Studies Unit of the Reactor Safety and Operational Analysis Department are gratefully acknowledged.

Table 1
Unit 1 Outage Heat Sinks 1995

Unit 1 Outage Heat Sink Configurations.

Planned	19-20 Sep	20Sep-5 Oct	5 Oct-6 Oct	6 Oct - 9 Oct	9 Oct -11 Oct	11 Oct -12 Oct	12 Oct 18 Nov	18 Nov -29 Nov	29 Nov - 6 De	6 Dec - 10 Dec	10 Dec - 18 Dec	18 Dec .. startup
Actual							18-Oct					
FDF /year	2.18E-05	2.33E-05	2.50E-05	2.64E-05	2.62E-05	7.85E-05	7.85E-05	8.11E-05	7.85E-05	2.82E-05	2.73E-05	2.17E-05
Duration	2	17	2	3	3	1	37	11	7	5	8	
S/D Days	2	19	21	24	27	28	65	76	83	88	96	100
Configuration	1	2	3	4	5	6	7	8	7	9	10	11
PHT System State	Full	Full	Full	Full	LLDS	LLDS	LLDS	LLDS	LLDS	LLDS	Full	Full
Moderator	Full in OPGSS	Full in OPGSS	Full in OPGSS	Full in OPGSS	Full in OPGSS	Full in OPGSS	Drained	Drained	Drained	Full in OPGSS	Full in OPGSS	Full
Primary Heat Sink	Shutdown Cooling	Shutdown Cooling	Shutdown Cooling	Maintenance Cooling	Maintenance Cooling	Maintenance Cooling	Maintenance Cooling	Maintenance Cooling	Maintenance Cooling	Maintenance Cooling	Maintenance Cooling	Shutdown Cooling
Alternate Heat Sink	Thermal Syphoning / Maintenance Cooling	Thermal Syphoning / Maintenance Cooling	Thermal Syphoning / Maintenance Cooling	IBIF to boilers	IBIF to boilers	IBIF to NPC	IBIF to NPC	IBIF to NPC	IBIF to NPC	IBIF to boilers	IBIF to boilers	Thermal Syphoning
PHT System Over Pressure Protection	CV20/21 to RV17/18	CV20/21 to RV17/18	CV20/21 to RV17/18	CV20/21 to RV17/18	RV16	Open boiler manways	Open boiler manways	Open boiler manways	Open boiler manways	RV16	CV20/21 to RV17/18	CV20/21 to RV17/18
Steam Drum 1	Boilers full	BO1, 2 drained. BO3,4 full.	BO1, 2 drained. BO3,4 full.	BO1, 2 drained. BO3,4 full.	BO1, 2 drained. BO3,4 full	BO1, 2 drained. BO3,4 full.	Boilers BO1,2,3,4, drained, steam drum open.	Boilers BO1,2,3,4, drained, steam drum open.	Boilers BO1,2,3,4, drained, steam drum open.	Boilers partially full steam drum closed	Boilers full	Boilers full
Steam Drum 2	Boilers full	BO5,78, full. BO6 maybe drained.	BO5,78, full. BO6 maybe drained.	BO5,78, full. BO6 maybe drained.	BO5,78, full. BO6 maybe drained.	BO5,78, full. BO6 maybe drained.	Boilers BO5,6,7,8, drained, steam drum open.	Boilers BO5,6,7,8, drained, steam drum open.	Boilers BO5,6,7,8, drained, steam drum open.	Boilers partially full steam drum open.	Boilers full	Boilers full
EBC	Available to both steam drums	Isolated to steam drum SD1	Unavailable	Available to both steam drums	Available to both steam drums	Available to both steam drums	Unavailable	Unavailable	Unavailable	Isolated to steam drum SD2	Unavailable	Available
Boilers Primary Side	Closed	Closed	Closed	Closed	Closed	Open	Open	Open	Open	Closed	Closed	Closed
Normal boiler feedwater system.	Available	Available	Available	Unavailable	Unavailable	Unavailable	Unavailable	Unavailable	Unavailable	Unavailable	Available	Available
EBC/MCS Jumper	Unavailable	Unavailable	Unavailable	Unavailable	Unavailable	Available	Available	Available	Available	Unavailable	Unavailable	Unavailable
Diesel Generator	Unavailable	Unavailable	Unavailable	Unavailable	Available	Available	Available	Available	Available	Available	Available	Available
SDS1	Available	Available	Available	Available	Available	Available	Shut-off rods in core.	Shut-off rods in core.	Shut-off rods in core.	Available	Available	Available
SDS2	Available	Available	Available	Available	Unavailable	Unavailable	Unavailable	Unavailable	Unavailable	Available	Available	Available
ECI	Blocked	Blocked	Blocked	Isolated	Isolated	Isolated	Isolated	Isolated	Isolated	Isolated	Isolated	Blocked
LPSW	Available	Available	Available	Available	Available	Available	Available	Unavailable	Available	Available	Available	Available
HPSW	Available	Available	Available	Unavailable	Unavailable	Unavailable	Unavailable	Unavailable	Unavailable	Available	Available	Available
Configuration	1	2	3	4	5	6	7	8	7	9	10	11
	2.18E-05	2.33E-05	2.50E-05	2.64E-05	2.62E-05	7.85E-05	7.85E-05	8.11E-05	7.85E-05	2.82E-05	2.73E-05	2.17E-05

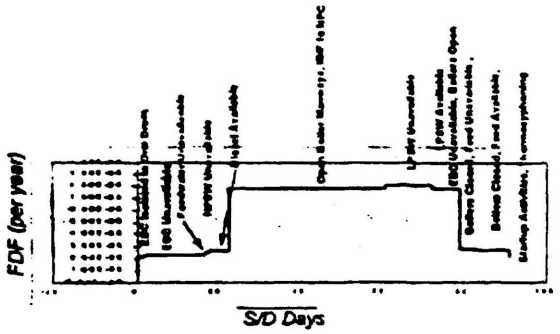
Table 3
unit 3 Outage Heat Sinks 1995.

Outage Start	03-Nov-95						
Unit 3 Outage Heat Sinks1995							
Planned	**7-Nov**	**8-Nov**	**9-Nov**	**10-Nov**	**18-Nov**	**19-Nov**	**23-Nov**
Actual							
FDF /year	**2.18E-05**	**2.45E-05**	**2.67E-05**	**2.91E-05**	**2.35E-05**	**2.17E-05**	**2.17E-05**
Duration	5	6	7	8	16	17	21
S/D Days	1	6	12	19	27	43	60
Configuration	**1**	**2**	**3**	**4**	**5**	**6**	**7**
PHT System State	Full	Full	**LLDS**	LLDS	LLDS	**Full**	Full
Moderator	Full in OPGSS	Full in OPGSS	Full in OPGSS	Full in OPGSS	Full in OPGSS	Full in OPGSS	Full
Primary Heat Sink	Shutdown Cooling	Shutdown Cooling	**Maintenance Cooling**	Maintenance Cooling	Maintenance Cooling	**Shutdown Cooling**	**Shutdown Cooling**
Alternate Heat Sink	Thermal Syphoning / Maintenance Cooling	Thermal Syphoning / Maintenance Cooling	**IBIF to boilers**	**IBIF to NPC**	**IBIF to boilers**	**Thermal Syphoning**	Thermal Syphoning / Maintenance Cooling
PHT System Over Pressure Protection	CV20 or 21 to RV17/18	CV20 or 21 to RV17/18	CV20 or 21 to RV17/18	CV20 or 21 to RV17/18	CV20 or 21 to RV17/18	CV20 or 21 to RV17/18	CV20 or 21 to RV17/18
Steam Drum 1	Boilers full	Boilers full	Boilers full	Boilers full	Boilers full	Boilers full	Boilers full
Steam Drum 2	Boilers full	Boilers full	Boilers full	Boilers full	Boilers full	Boilers full	Boilers full
EBC	Available to both steam drums	Available to both steam drums	Available to both steam drums	**Not Needed** Available to both steam drums	Available to both steam drums	Available to both steam drums	Available to both steam drums
Boilers Primary Side	Closed	Closed	Closed	**Open**	**Closed**	Closed	Closed
Normal boiler feedwater system.	Available	**Unavailable**	Unavailable	Unavailable	**Available**	Available	Available
EBC/MCS Jumper	Unavailable	Unavailable	Unavailable	**Available**	**Unavailable**	Unavailable	Unavailable
Diesel Generator	Unavailable	Unavailable	Unavailable	**Available**	[illegible]	**Not Required**	[illegible]
SDS1	Available	Available	Available	Available	Available	Available	Available
SDS2	Available	Available	Available	Available	Available	Available	Available
ECI	Blocked	Blocked	**Isolated**	Isolated	Isolated	Isolated	**Blocked**
LPSW	Available	Available	Available	Available	Available	Available	Available
HPSW	Available	Available	Available	Available	Available	Available	Available

Graphs

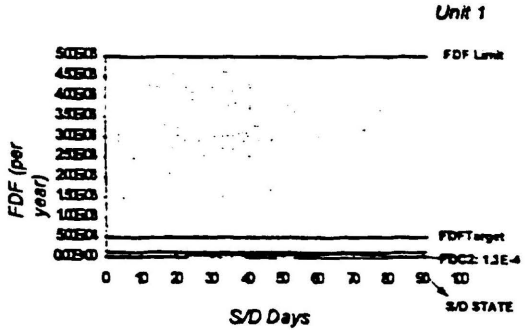
FDF vs. S / D days plot Unit 1

Unit 1



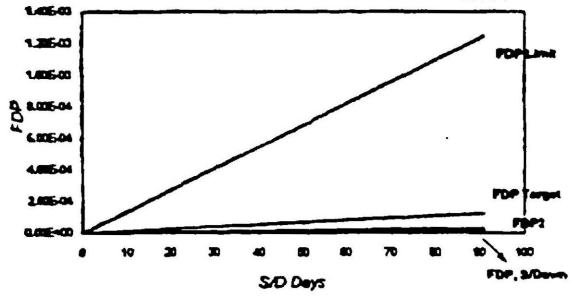
FDF vs. S / D days plot Unit 1

Unit 1

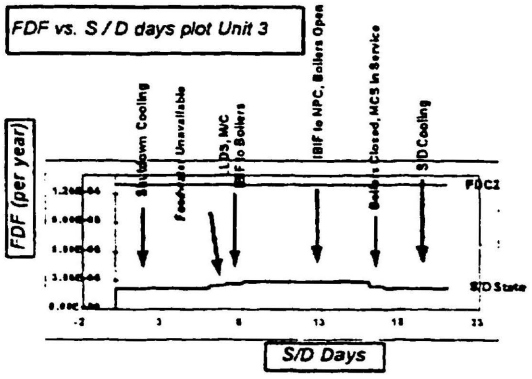


Fuel Damage Probability Plot
FDP Vs S / D Time

Unit 1

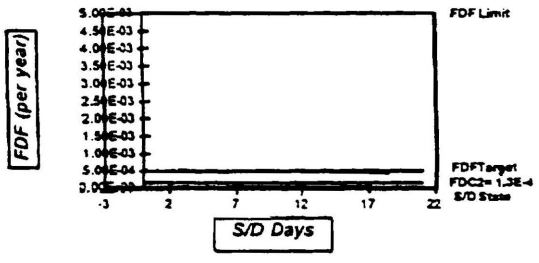


FDF vs. S / D days plot Unit 3



Fuel Damage Frequency Plot
FDF vs S / D Time

Unit 3



Fuel Damage Probability Plot
FDP vs S/D Time

Unit 3