Development and Application of an Operational Probabilistic Risk Assessment (PRA) at Ontario Power Generation

S. Kaasalainen, J. Mok, K. Donnelly, K. Dinnie
Nuclear Safety Solutions Ltd.
Toronto, Ontario, Canada

S. Ganguli, M. Moisin
Ontario Power Generation Inc.
Pickering, Ontario, Canada

ABSTRACT

Ontario Power Generation Inc. has embraced the use of Probabilistic Risk Assessment (PRA) in operational decision-making. Common examples include decisions related to continued operation while in an abnormal plant configuration based on incremental risk increase, and the use of risk monitors (i.e., Equipment Out-of-Service (EOOS)) for outage planning and managing risk during on-line maintenance. Unlike the baseline PRA where average risk is calculated, these operational decisions/tools are best made using a real-time, or instantaneous analysis reflecting actual plant configuration. The process of taking the baseline, time-averaged PRA, to an instantaneous model is part of broader process of "operationalizing" the plant PRA. Additional items in the process include activities related to the development of the risk monitors themselves, and the development and establishment of procedures and governance related to the use of the PRA and risk monitors in applications. This paper looks into the processes and factors requiring consideration when "operationalizing" a nuclear power plant PRA. As well, the paper includes a case study describing the use of an operational PRA to support the decision-making process at Pickering NGS B.

INTRODUCTION

The Probabilistic Risk Assessment (PRA) program at Ontario Power Generation Inc. (OPG) has been developed in the context of supporting operating power plants. As such, the primary objective has always been to enable the use of risk-informed decision-making related to plant operations and maintenance. The result was the development of a PRA methodology optimized for the development of an Operational PRA model. The OPG approach to "risk-informed" decision-making was initiated well before, and independent of, risk-informed elements of the regulatory framework and/or regulatory requirements, for example, S-294 (Reference 1).

There are a number of alternative approaches and tools available for developing a nuclear power plant PRA. For example, it is common industry practice to utilize an event tree/fault tree approach, however, the boundaries related to what parts of the model are included in the event trees vs. fault trees is subject to a significant degree of variation between studies. A key factor in choosing the PRA methodology lies in the planned applications for the study when completed. That is, a PRA developed as a design or licensing study may utilize different methodologies compared to a PRA being developed for use in an operational setting. That is not to say that a design, or licensing, PRA cannot be used in an operational setting, however, the extent to which the model would require modification in order to make it convenient for use in an operational setting may be greater than if the model had been built from the perspective of an operational PRA from the outset.

Key elements of the OPG operational PRA program include the development and maintenance of the time-averaged baseline PRA models, adaptation of the baseline models to instantaneous models, development and implementation of risk monitors, and development and implementation of governance to provide a framework for risk-informed decision-making. Each of these items is briefly discussed in the present paper. This somewhat generic discussion is followed by an example, or case study, of a risk-informed decision made at the Pickering NGS B power plant using the operationalized version of the Pickering B Risk Assessment (PBRA).

THE BASELINE PRA

The main input into the development of an operational PRA, is an up-to-date time-averaged baseline PRA model. The development and maintenance of a baseline PRA is not a small task, and is where the majority of PRA resources are utilized. Although this paper is not related to the subject of development and maintenance of the baseline PRA, there are some approaches that can be adopted in the development of the baseline PRA that will facilitate the production of the operational PRA – hence, providing savings and efficiencies in terms of the resources and schedule.

For instance, consider the quantification or integration step of the PRA. It is common to utilize a sequence-by-sequence type of quantification technique. That is, each sequence of the event trees are integrated with the relevant fault trees and quantified one-at-a-time. The cutsets from each sequence are then obtained and analysed separately. The final result, in terms of minimal cutsets leading to a similar end state (i.e., fuel damage and ex-plant release categories) is obtained by combining the cutsets for each sequence leading to the same end-state. This approach works well for generating the time-averaged solution, but is not necessari;y the most efficient process in the context of an operational PRA, or risk monitor, as it involves a large number of separate and independent calculations which need to be combined in order to re-calculate the end-state or risk metric of interest. Ideally, for purposes of a risk monitor, a fully integrated fault tree is developed with the top event representing the risk metric of interest. This enables quick and automatic re-quantification of the risk metric for any given plant configuration.

At OPG, the baseline PRA solution is obtained by first converting the event tree logic into high level fault tree logic for each fuel damage category and ex-plant release category, then integrating the high level fault trees with the system level fault trees. In this way, a top logic model is developed for each end-state. This top logic model is then available for use directly in the operational PRA, or risk monitor, which is, as stated above, the desired form for the PRA for use in a risk monitor.

As a second example, consider a train based system. It is typical in a PRA model to have one train assumed to be in-service and the second train assumed to be on standby. On a time-averaged basis it does not matter which train is selected for in-service and which is selected for standby. However, in an instantaneous (or operational model), the objective is to specify precisely the configuration of the plant – hence, it would be useful to have the option of selecting either train to in-service. Resolving this type of asymmetry can be done in the baseline time-averaged model, or can be done as a separate step as part operationalizing the PRA. Currently, at OPG, this is addressed by manual manipulations of the model.

THE OPERATIONAL PRA

An operational PRA is "a plant specific real-time analysis tool used to determine the point-in-time risk which is based on the actual plant configuration defined in terms of the Plant Operational Mode, the components that have been removed from service, the choice of running and standby trains for normally operating systems and setting other environmental factors." (Reference 2).

The basis of the operational PRA is the baseline, time-averaged PRA with modifications typically made to address the following:

- Remove some of the simplifications made in the baseline model (i.e., resolve the modelling asymmetries as needed);
- Remove any time-averaged test and maintenance events (i.e., the reference operational model should be reflective of zero maintenance);
- Remove any time-averaged conditional events (for example, environmental conditions) and replace them with true or false settings (i.e., it is known if the conditions are true or not);

As a result of the modifications to the time-averaged baseline PRA, the quantitative results associated with the instantaneous, operational model will be different from those reported in the baseline time-averaged model. As an example, consider the severe core damage frequency predicted for Pickering NGS B. The time-averaged value for the at-power state is predicted to be about 1.0E-5 occ./yr, whereas the zero maintenance, instantaneous value is predicted to be about 7.5E-6 occ./yr using the same truncation value (E-11). It is important to validate this difference in the context of the changes made to the models. In this case, the difference in the quantified results are due largely to the removal of the test and maintenance events.

THE RISK MONITOR

With an instantaneous, zero maintenance PRA model developed, the main infrastructure associated with a risk monitor is complete. In fact, valid risk-informed decisions can be made using this model without the aid of a risk monitor. However, generally speaking, manipulation of the model would most often require an amount of skill and knowledge of PRA that is beyond the expectation of most plant staff. The main purpose, then, of the risk monitor is to enable the use of the station risk assessment, by staff other than the PRA group. A risk monitor enables this by overlaying the PRA with a user friendly interface.

At OPG, the risk monitor software used is the EPRI Risk and Reliability Workstation tool EOOS (Equipment Out-of-Service). OPG has risk monitors developed for the at-power and outage states. Figure 1 illustrates the "operators" status panel of the Pickering NGS B At-Power Risk Monitor.

Figure 1 illustrates the zero maintenance configuration (i.e., no equipment out-of-service). On the upper left corner is the "risk meter" which shows the instantaneous severe core damage frequency. With no equipment out-of-service, the Pickering B severe core damage frequency is predicted to be 7.5E-6 occ./yr.

To the right of the risk meter is a list of equipment currently out-of-service (empty in Figure 1 as no equipment is removed from service). Across the bottom of the screen are the "status" panels providing deterministic information regarding the availability of selected systems. The selection of systems to be shown as status panels is customized according to the particular station needs and desires.

Figure 2 provides an example of the instantaneous risk at Pickering NGS B with a piece of equipment taken out-of-service. In this example, valve 5-7138-V82 is removed from service rendering the make-up water from the Emergency Storage Water Tank (ESWT – or the Dousing Tank) at the top of the vacuum building to the moderator unavailable. The result is a loss of the moderator boil-off heat sink, which is credited as a long-term mechanism of decay heat removal. Clearly, this change has an impact on the instantaneous severe core damage frequency (as shown in the risk meter). As well, the associated status panels have turned red indicating the unavailable status of the emergency water supply to the moderator.

The EOOS monitor also provides a second screen for the so-called "scheduler". An example, from the Pickering B at-power risk monitor is shown in Figure 3. The scheduler screen enables a review of the risk profile of various proposed plant configurations before they are implemented. This is particularly useful for outage planning as a tool for checking and optimizing the risk profile of an upcoming outage.

A FRAMEWORK FOR RISK-INFORMED DECISION-MAKING

Up to now the focus of this paper has been on the development of the operational PRA and risk monitors. To use the risk monitor for decision-making a framework must first be established to provide the criteria for making decisions.

At OPG a number of standards and guidelines have been developed to guide station staff with using the PRA in the context of operational decision-making. An example is the OPG Guideline for Management of Incremental Risk from Abnormal Plant Configurations. This document provides guidance for managing incremental risk from abnormal plant configurations to ensure the following:

- The configuration does not cause the plant to operate at an unduly high risk level even for a short period of time;
- The resulting incremental risk does not cause the relevant safety goal limits to be exceeded;
- Adequate guidance is in place to manage risk while operating in an abnormal configuration; and
- Any long-term implications or actions are identified and accounted for.

The overall process is risk-informed in that it uses quantitative estimates of risk to determine the risk management guidance applicable to a given plant configuration, but places some deterministic restrictions on the maximum durations of such configurations.

The guideline utilizes the concepts of “instantaneous” risk and “incremental” risk for quantifying risk impacts. In this context, instantaneous risk is defined as the risk calculated for a specific plant configuration assuming duration is indefinite, whereas incremental risk is the calculated risk increase (or increment) from the average baseline risk for a specific plant configuration.

The guideline considers four sets of circumstances as follows:

- The configuration is planned, is of known duration, and is covered by the plant PRA. In this case a direct calculation of instantaneous risk and incremental risk can be obtained;
- The configuration is planned, of known duration but is not covered by the plant PRA. In this case an instantaneous risk estimate using a separate analysis, supplementary to the plant PRA is required. Incremental risk is then the instantaneous risk multiplied by duration;
- The configuration is unplanned but does not impact the design basis (i.e., is temporary). In this case, instantaneous risk is calculated directly from the plant PRA (or supplementary analysis if necessary), and allowable durations are determined by comparing with incremental risk limits established in the guide;
- The configuration is unplanned and leads to a change in the design basis (configurations of this type should get added to the plant PRA at next update). In this case, instantaneous risk generally cannot be calculated directly from the plant PRA, but may be calculated by means of supplementary analysis. Allowable durations are determined by comparing with incremental risk limits established in the guide.

The process outlined in the guideline is illustrated below by means of a case study.

CASE STUDY

A concern had been raised at Pickering NGS B regarding how best to deal with a hypothetical events of a spurious opening of the panels associated with the Powerhouse Emergency Venting System (PEVS) panels under an extreme cold winter weather condition. If such an event were to occur, equipment residing in the powerhouse could freeze. This could have economic as well as safety implications.

One option considered for dealing with this issue was to instruct operations to force close the PEVS panels if they were to spuriously open. However, force closing the PEVS panels would render the system unavailable for performing its design function (i.e., to mitigate the consequences of a steam line break).

In order to quantify the risk impact of force closing the PEVS panels following a spurious opening, PBRA was used in conjunction with the OPG Guideline for Management of Incremental Risk from Abnormal Plant Configurations.

Using severe core damage frequency as the risk metric of interest, a calculation of the incremental risk associated with plant operations with the PEVS system disabled was performed using the instantaneous EOOS model.

The baseline risk is 1.0E-5 occ./yr. With PEVS taken out-of –service this value increased to about 2.0E-4 occ./yr (i.e., the instantaneous risk). The incremental risk, then, is 1.9E-4 occ./yr (i.e., 2.0E-4 – 1.0E-5 occ./yr).

Based on the guideline, planned configurations would not normally be entered if the incremental core damage probability (ICDP) exceeds 1E-5. ICDP is calculated from the incremental core damage frequency (ICDF) times duration of the planned configuration. Thus, using the ICDP limit of 1E-5, and the calculated ICDF of 1.9E-4, an allowable duration of 0.053 years (19 days) was calculated (i.e., 1E-5/1.9E-4).

SUMMARY

OPG and NSS have worked collaboratively to develop the infrastructure associated with the use of operational PRAs for decision-making related to plant operations and maintenance. The steps associated with this process have involved the development and maintenance of the time-averaged baseline PRA models, adaptation of the baseline models to instantaneous models, development and implementation of risk monitors, and development and implementation of governance to provide a framework for risk-informed decision-making. Because OPG developed the PRA program with plant operations in mind from the outset, the use of the PRA in application has influenced the choice of tools and methodologies for PRA development, the result being a PRA program optimized to the needs of operating plants.

REFERENCES

1. Canadian Nuclear Safety Commission, Regulatory Standard, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, S-294, April 2005.

2. NEA/CSNI/R(2004)20, Risk Monitors, The State of the Art in their Development and Use at Nuclear Power Plants.

Figure 1: Screenshot of the Operator Screen of the Pickering NGS B At-Power Risk Monitor (EOOS) – Zero Maintenance Condition

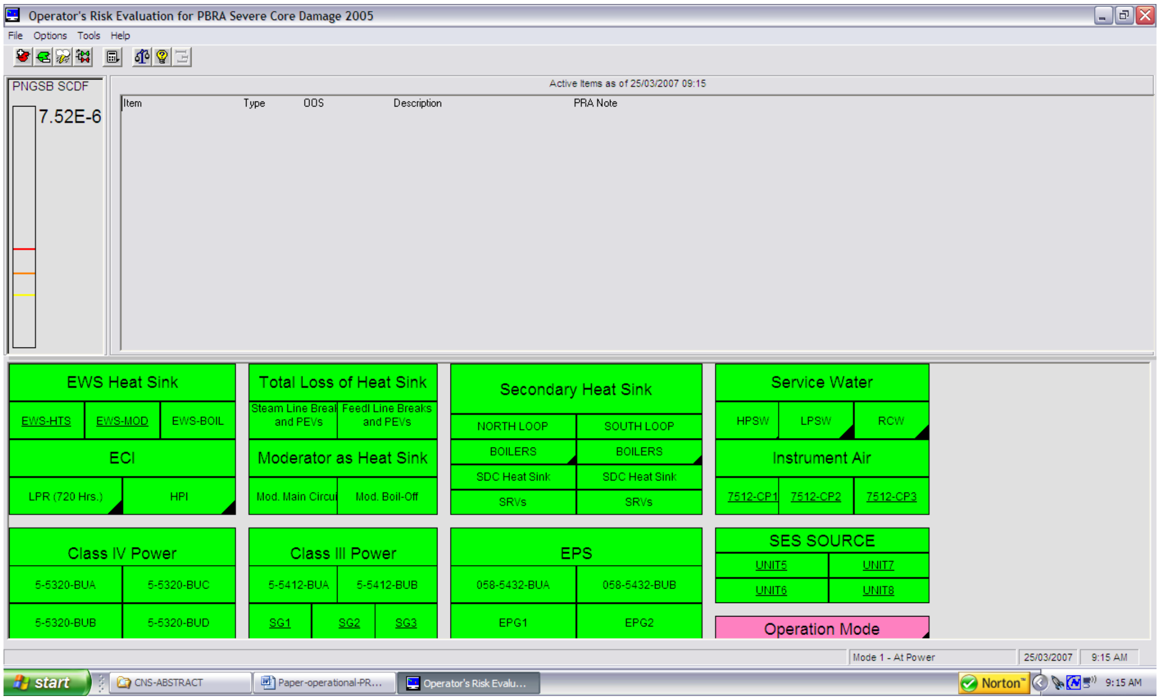
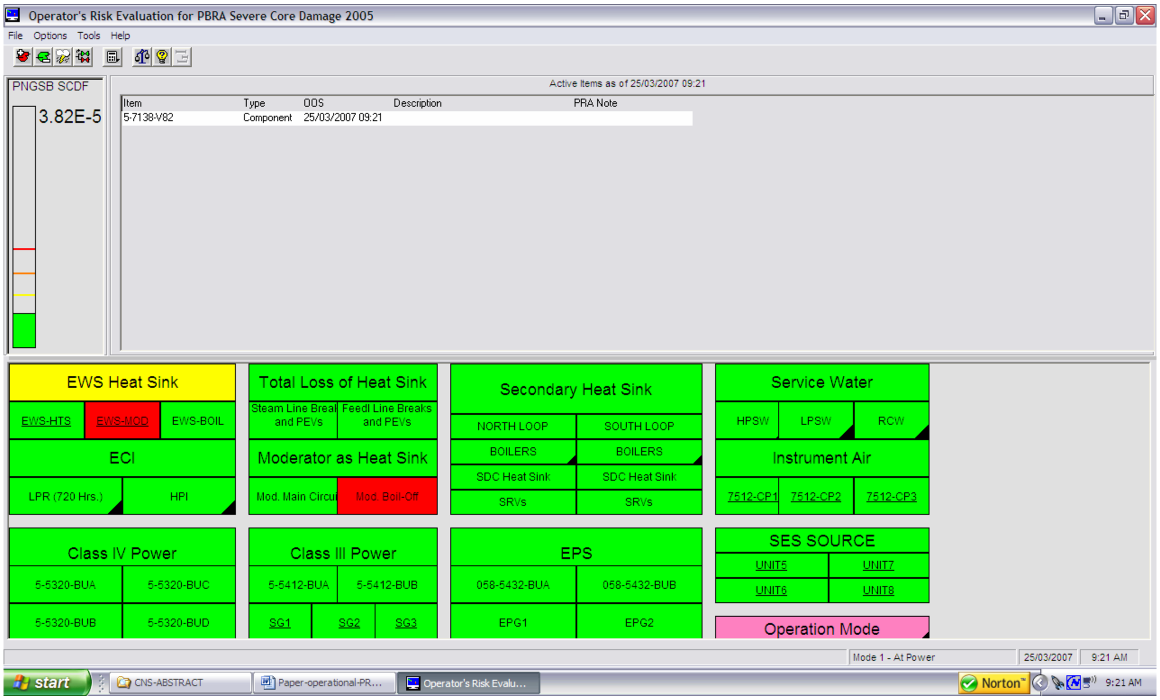


Figure 2: Screenshot of the Operator Screen of the Pickering NGS B At-Power Risk Monitor (EOOS) – Valve 5-7138-V82 Out-of-Service



Operator's Risk Evaluation for PBRA Severe Core Damage 2005

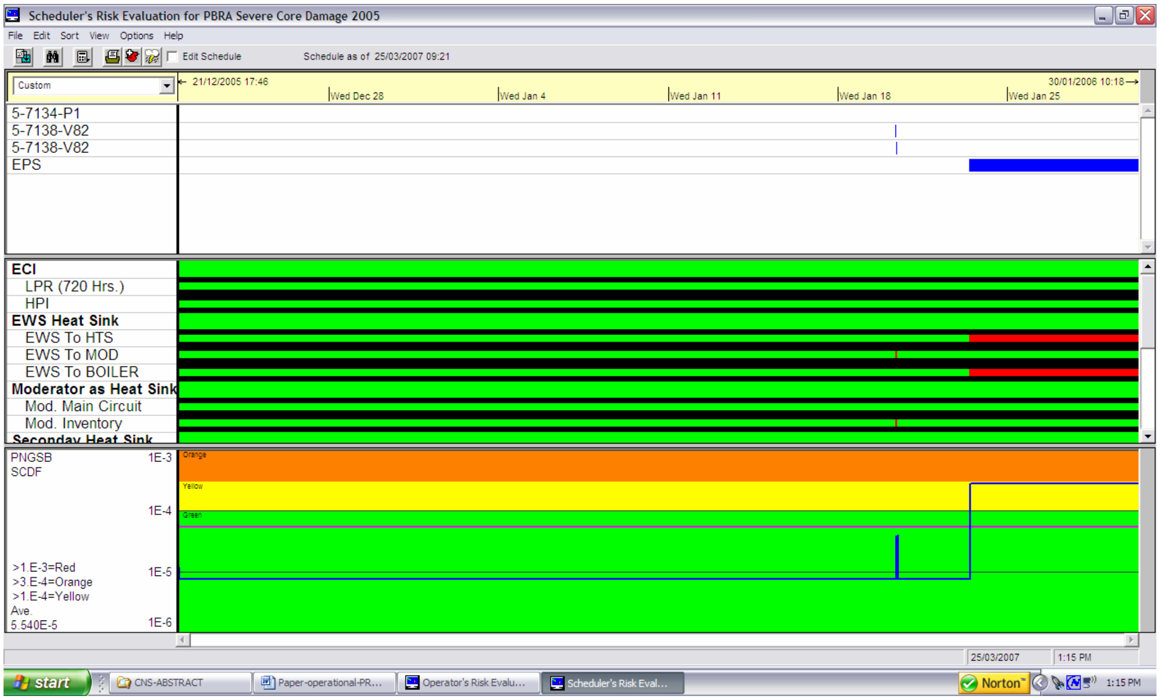
PNGSB SCDF 3.82E-5

Active Items as of 25/03/2007 09:21

Item	Type	OOS	Description	PRA Note
5-7138-V82	Component	25/03/2007 09:21		

Mode 1 - At Power 25/03/2007 9:21 AM

Figure 3: Screenshot of the Scheduler Screen of the Pickering NGS B At-Power Risk Monitor (EOOS)


Scheduler's Risk Evaluation for PBRA Severe Core Damage 2005
File Edit Sort View Options Help
Edit Schedule
Schedule as of 25/03/2007 09:21
Custom
← 21/12/2005 17:46
Wed Dec 28
Wed Jan 4
Wed Jan 11
Wed Jan 18
Wed Jan 25
30/01/2006 10:18 →
5-7134-P1
5-7138-V82
5-7138-V82
EPS
ECI
LPR (720 Hrs.)
HPI
EWS Heat Sink
EWS To HTS
EWS To MOD
EWS To BOILER
Moderator as Heat Sink
Mod. Main Circuit
Mod. Inventory
Secondary Heat Sink
PNGSB
SCDF
1E-3
1E-4
1E-5
1E-6
>1.E-3=Red
>3.E-4=Orange
>1.E-4=Yellow
Ave.
5.540E-5
Orange
Yellow
Green
25/03/2007
1:15 PM
start
CNS-ABSTRACT
Paper-operational-PR...
Operator's Risk Evalu...
Scheduler's Risk Eval...
Norton
1:15 PM