EXPERIENCE WITH PRA APPLICATIONS IN ONTARIO HYDRO NUCLEAR

V.M. Raina
Ontario Hydro, Canada

ABSTRACT

Ontario Hydro has carried out probabilistic risk assessments (PRAs) for a number of its nuclear generating stations, comprising detailed fault tree models of various safety-related plant systems, component failure data bases, and in-plant and ex-plant consequences of severe accidents. The PRA s have frequently been used to support plant operation in areas such as assessment of safety impact of forced equipment outages, maintenance planning, prioritization of systems and components for resource allocation, and reliability assessments of design backfits.

This paper provides details of a number of such applications. For each application it describes the issues of concern, the evaluation method, and the manner in which PRA results were used in issue resolution.

INTRODUCTION

As part of its program of plant-specific probabilistic safety assessments, Ontario Hydro Nuclear (OHN) has developed detailed fault-tree based models for various safety-related systems. Also developed is the high level logic that links the system models to provide sequences of events that may lead to core damage and release of radioactivity to the public. The availability of integrated logic models that relate component failures and operator errors to core damage and off-site release has led to these models, or the information contained in them, being used to assist in operational decision-making. The purpose of this paper is to provide some examples of these applications.

In broad terms, applications of PSAs to date may be categorized into the following:

a) Assessment of safety impact of equipment outages;

b) Scheduling of planned maintenance activities to appropriately control plant risk;

c) Prioritization of systems and components; and,

d) Assessment of adequacy of design modifications.

SAFETY IMPACT OF EQUIPMENT OUTAGES

By far the largest use of the risk models has been in evaluating the risk impact of equipment outages to help determine appropriate compensatory actions. For each of the following cases, the situation experienced is described, the issues facing the decision-maker are presented, and some details are provided of the information extracted from the risk models to help in the decision-making.

Case 1

At one of OHN's generating units, one liquid zone pump, forming part of the unit's reactivity control system, has failed and is unlikely to be repaired until the next planned outage which is a few months away. The failed pump is one of three redundant pumps and is supplied from the so-called even power supply. Each of the remaining pumps is supplied from a separate power bus belonging to the odd power supply division. It is proposed to put in place a temporary arrangement (jumper) by means of which one of the

remaining pumps would be powered from an even power supply instead of its normal odd supply. This would prevent the liquid zone system from failing if the odd power supply were to be lost over the outage duration of the failed pump. Failure of the liquid zone system leads to a reactor shutdown and also has the potential to initiate an accident involving uncompensated positive reactivity insertion should other mitigating actions fail, such as closure of the liquid zone compartment drain valves on low pump discharge pressure. The question is raised as to whether it is worthwhile from a safety point of view to implement the proposed jumper.

The logic model for the event "Loss of water supply from the liquid zone pumps AND failure of the drain valves to close" contained in the plant's risk assessment was used to assess the significance of the loss of one of the liquid zone pumps as well as the potential benefits from the proposed jumper. The model for this event was built up from models for the various systems which could affect the occurrence frequency of the event of interest, chief among which were the reactor regulating system, the electrical power system, and the digital control computer system.

The assessment showed that the major contributors to the draining of the liquid zone compartments involved failures in which both divisions of the relevant electrical power supply were affected. These were events involving losses of the bulk electricity system (BES) or dual computer failures in conjunction with a turbine trip. Events in which both buses in the odd power supply division had failed were not only few in number but also of low frequency. The increase in failure frequency in the absence of the beneficial effects of the jumper was only about one tenth of the normal or base-line frequency. The frequency of the affected contributors to the draining of the zone compartments did increase by an order of magnitude; however, this value was already very low compared to other causes of failure. It was, therefore, concluded that there was not a significant benefit in changing the source of the power supply to one of the available pumps.

The assessment also pointed to the potential for human error in changing to a non-standard power supply configuration. For example, supplying one of the normally odd-powered pumps from the failed pump’s supply would have required leaving the latter's control handswitch in the main control room in the standby position. The possibility could, however, exist that this handswitch would be inadvertently selected to the off position at some time during the outage on the assumption that an out-of-service pump's control handswitch should be selected off. This would result in running pump failure leading to loss of water supply to the zone compartments.

An insight provided by the assessment was that even though hardwired logic had been provided to close the zone compartment drain valves on loss of water supply as a backup to similar action taken through the control computer system, failure of the computer system, nevertheless, led to failure to prevent the zones from draining. This arose from the fact that even though the computer system alone was not relied upon to close the drain valves, it was required to operate in order to prevent the sudden opening of these valves, and, hence, draining of the zones, once water pressure was restored.

Case 2

The 250v DC power distribution system in OHN's generating units, typically, comprises redundant odd and even power buses, with each bus supplied by two redundant rectifiers. In one of the units, one even and one odd rectifier have failed simultaneously. In addition, there is some concern about the ability of an operating rectifier to carry the entire load should the other rectifier fail. A decision needs to be made on continued operation in this state until the failed rectifiers can be brought back into service.

To assist in the required decision-making, the plant's risk model was used to assess the risk impact of the encountered operating configuration. The nuclear safety significance of the failed equipment arises from the fact that loss of the 250v DC system can potentially impair a number of different means of fuel cooling, viz., the boiler feedwater system, the shutdown cooling system and the maintenance cooling system. An

assessment was, therefore, carried out of the effect of the given component failures on the likelihood of loss of the above three redundant cooling systems.

Two subcases were analyzed. In one, each of the remaining rectifiers was assumed to be capable of carrying the entire load, while in the other it was assumed that failure of either rectifier would lead to failure of the other operating rectifier as well due to overload. The assessment considered the increased likelihood of DC distribution system failure both initiating an accident sequence as well as affecting accident mitigation. For the first subcase, an increase in loss of heat sink frequency of about a factor of 2 was assessed, while in the second, the increase was a factor of 6. While the former is not significant, the latter was such that it needed to be factored into the decision-making process. It was decided that while operation of the reactor with one odd and one even rectifier out of service could continue, the reactor would be shutdown in a controlled manner in the event that either operating rectifier exhibited signs of reduced capability.

Case 3

At one of OHN's plants the following equipment is out of service while operating at power: a main boiler feedwater pump, a closed loop de-mineralized service water (CLDSW, nuclear component cooling water) pump, and a low pressure service water (LPSW) pump. The affected components are parts of systems that have a role in the maintenance of reactor heat sink. At the same time, a routine test on a pump in the emergency service water system (EWS) has become due for execution. The EWS system provides an emergency supply of water to the steam generators in the event that all other means of decay heat removal are lost. The operators are faced with the question of whether, given the equipment outages, it is wise to make one of the emergency service water pumps unavailable due to the test. The decision is made not to carry out the test as planned. The question then arose: what would have been the impact on risk if the test had been done? Importantly, should operating procedures be modified to preclude this test if similar conditions are experienced in future.

The plant's risk model was queried to determine the risk impact. Since the main issue is heat sink reliability, the contributors to loss of heat sink contained in the plant model were re-assessed with the subject pump outages incorporated. The results were compared with the base-line heat sink failure frequency estimates in which failure probabilities of the out-of-service pumps were assigned their nominal values. With all contributors taken into account, including those not affected by the equipment outages, the heat sink failure frequency was calculated to be increased by a factor of 1.5, which is a relatively small increase.

The reason for the small difference between the nominal and the modified case was due to the fact that the dominant contributors to loss of heat sink frequency are those events that affect whole system(s). For example, a major cause of loss of the boiler feedwater and backup maintenance cooling systems is the loss of low pressure service water resulting from failure to isolate required LPSW loads following a loss of the BES and failure of the unit to survive the BES loss, rather than coincident failure of feedwater and maintenance cooling pumps. Likewise, the EWS supply to the steam generators is more likely to fail due either to failure to valve it in when required, or inability to open the supply valve in the line between the steam generators and emergency water system.

To obtain a different perspective on the problem, the impact on only those contributors to heat sink failure that contained the affected components was also assessed. A factor of 2.6 increase was estimated. As expected, the difference between this and the base-line case was higher than in the case in which all contributors were included, although not by a significant amount. (In probabilistic terms, increases by factors less than 3 are not particularly significant.) The reason that the impact was still small is that there is considerable component redundancy in each of the affected systems. For example, even with one boiler

feedpump out of service, two main and one auxiliary boiler feedpump are still available to provide feedwater to the steam generators to remove decay heat.

It was, therefore, concluded that from risk considerations it would be acceptable to undertake testing of an EWS pump with one pump each being out-of-service in the LPSW, CLDSW and boiler feedwater systems.

MAINTENANCE PLANNING

Ontario Hydro has used its PRA models on a number of occasions in decisions related to maintenance. The central idea behind the application of PRA models in maintenance is to ensure to the extent possible that maintenance activities do not result in unduly large increases in plant risk, typically measured by frequencies of various levels of fuel damage. Risk due to maintenance can be assessed both if the maintenance occurs at power or during an outage. Because of the large items of equipment that can become unavailable during a planned outage, and the difficulty thereof of assessing safety impact simply by inspection, the use of risk models to outage planning has aroused particular interest. The risk models provide a means of identifying the risk associated with various outage configurations before equipment is actually taken out of service. Should any high risk configurations be uncovered, maintenance activities can be re-arranged to eliminate such configurations.

Most PRA models are developed to assess the risks associated with high power operation. In order to use PRA methods to assess outage risk, it is necessary to have available a so-called outage risk model for the plant to reflect the different accident initiation and mitigation, and equipment outage, possibilities. Such models can, however, be conveniently and efficiently derived directly from the at-power models. In Ontario Hydro, outage risk models are now developed in conjunction with the at-power models.

The use of PRA models for assessing planned outages also imposes a requirement for integrating outage schedules with the PRA so that changes in outage plans can be easily reflected in the models. It is also important that the outputs of the PRA be presented in a readily-reviewable form, such as in the form of a plot of risk against time. Furthermore, the number of configuration changes during an outage can be quite large, in the order of 30 to 50. The ability must, therefore, exist to quickly calculate the risk for each configuration encountered during the outage. Ontario Hydro has acquired the computer tool called EOOS, for equipment out of service, developed by Science Applications Incorporated with the support of the Electric Power Research Institute (EPRI), to carry out such interrogations in conjunction with the OHN fault tree solution package.

In the following, two examples are presented of decision-making related to maintenance in which risk methods and tools were utilized. The first describes an application of the outage risk model and the second an at-power maintenance issue.

Case 1

During an upcoming planned outage it is intended to undertake maintenance on a number of heat transport (HT) system components. As a result, various operational states of the HT system will be entered, ranging from the system being closed, open to containment for steam generator maintenance, and open outside containment for HT pump maintenance. Among equipment to be removed for service are the emergency coolant injection valves, emergency water supply valves to the steam generators, and various electrical power buses. An outage plan has been developed for carrying out the maintenance work, resulting in about 40 different state changes. It is desired to know the risk associated with each state, i.e., the risk profile during the outage.

To calculate the risk profile, the outage risk model for the facility was implemented on the EOOS tool. Data on component outages was entered in terms of maintenance start and end dates. For each operating state and component outage, relevant fault tree failure events were identified, which were set to the certain (occurred) state.

The resulting risk profile showed a large risk increase relative to other outage states for the configuration in which, among other items, valves in the EWS supply lines to the steam generators were under maintenance. Test cases were then run in which the EWS outage state was shifted to different times during the outage. The EOOS tool allows such cases to be run by simply moving on the computer screen the selected component outage to any point in the outage. Significant reductions were achieved by moving the EWS outage to a different time slot during the outage.

Before accepting the results from any computational tool it is important to understand the reasons behind the model prediction. In the case assessed, the reduction in risk was achieved by moving the EWS outage to those periods in time in which the HT system was open rather than closed. With the system closed, the backup heat sink to loss of maintenance cooling is heat removal by means of the steam generators. EWS outage during this period removes one way of supplying water to the steam generators, and, hence, reduces the backup heat sink reliability. On the other hand, if a loss of heat sink were to occur during the time the HT system is open, an alternative way of core cooling is available in which coolant can be injected into the HT system and discharged from the HT opening. It is, thus, risk-beneficial to schedule the EWS outage such that it takes place when the HT system is open for maintenance. While such reasoning could have been applied even in the absence of the risk model, the risk tool spurred the search for an alternative strategy, pointed to a possible alternative, and graphically demonstrated its benefit.

Case 2

Planned maintenance of auxiliary moderator pumps is carried out at power. Normally, the two auxiliary moderator pumps are selected to the standby state to start automatically should the main moderator pumps fail. However, there is concern that if during maintenance of an auxiliary pump, the other auxiliary moderator pump automatically starts there will be increased radiation dose to workers, which can be avoided if the pump is turned off during the maintenance work. The decision to be made is whether it is acceptable to maintain a moderator pump with the second auxiliary moderator pump's handswitch selected to the off state.

To obtain some guidance on this issue, reference was made to the risk models, and the impact of the operational change on core damage frequency assessed. Auxiliary moderator pump failures affect core damage in two ways, viz., by potentially reducing the reliability of the moderator heat sink, and by making more likely the frequency of loss of moderator cooling initiating event requiring reactor shutdown. The risk models were used to calculate the increase in core damage frequency contribution of the above types of sequences due to the changed auxiliary moderator pump status. The time available for switching the pump's handswitch back to the standby state was determined (about 30 minutes) and the likelihood of the operator failing to do so in a timely manner evaluated.

The assessment showed that provided adequate pump recall procedures were put in place to minimize the likelihood of operator error, and the non-outage pump was tested prior to commencing the maintenance work to reduce the likelihood of undetected hardware failures, the increase in core damage frequency was negligible (about 3%). The reduction in maintainer risk was also evaluated and found to be about a factor of 2. Thus, the maintenance work could proceed with the available auxiliary moderator pump turned off.

PRIORITIZATION OF SYSTEMS AND COMPONENTS

While the optimum allocation of resources among competing contenders is of critical importance in the operation of any industrial facility, it is especially so in the case of nuclear power plants. This derives from their complexity as well as the stringent safety requirements to which they are subject. Resource allocation strategies in nuclear utilities must be such that public risk is adequately and consistently controlled. Appropriate resource allocation strategies would direct resources to systems and components with the most risk significance. Risk assessments provide a means of identifying the most important systems and

components with respect to public risk. It is, thus, natural to explore the use of risk assessments in resource allocation.

In Ontario Hydro Nuclear, a program of importance from the point of view of ensuring that resources are expended where most needed is the environmental qualification program. The purpose of the EQ program is to ensure that systems and components required to mitigate the consequences of an accident are capable of operating in the presence of the harsh environment that may exist following the accident. Risk assessments have been used to guide to the extent feasible the conduct of this program as demonstrated by the following example.

Case 1

With the prospect of delays in the EQ program, questions were asked as to the risks of operating without the EQ program fully in place and whether the qualification work on systems and components was being conducted in an order consistent with their risk reduction potential. It was desired to apply risk assessment methods and models to the problem at hand.

The application of risk assessments to the EQ issue presents both modelling and data problems, in that there are uncertainties as to which plant components are affected, in what way, and what is the likelihood of failure. Furthermore, EQ risk assessments need to recognize the common mode nature of the initiating event and the potential for redundant systems to be simultaneously affected.

To make the analysis tractable, a simple risk model was developed in terms of system level failures, based on insights from detailed risk models, with the possibility of system failure due to lack of EQ explicitly included as a contributing cause. This allowed three modes of interest to be simulated by assigning appropriate probability values depending on a system's expected or intended level of EQ, viz., a value of 1 for total lack of EQ, a value of 0 for full EQ, and a non-zero value for partial lack of EQ based on judgment and expert opinion. The risk model reflected all key plant safety attributes and credits, and provided as its output failure frequencies of individual early fatality, individual delayed fatality, large off-site release, and core damage frequency, which could be compared against OHN's risk-based safety goals. Further, it also considered the possibility that if two redundant systems were exposed to the same environment, the likelihood of their failure was strongly correlated.

The risk models determined, based on judgments as to system survival in a harsh environment, that by and large the effect of lack of formal EQ was to place plant risk in the so-called value impact region of OHN's nuclear safety goals. This meant that to the extent model assumptions and credits were not violated, the plant could continue to operate while the EQ program was expeditiously implemented. The models also identified modifications to mitigating systems which ought be the engineered first, viz., the powerhouse venting system to control the effects of a steam line break. Furthermore, a number of sensitivity studies were undertaken to determine the impact of qualifying various systems at different points in time. The assessment stressed the benefits of prioritizing qualification activities such that confidence could be gained that the moderator heat sink would operate if required in the event of a harsh environment in the reactor building, to reduce the likelihood of core damage.

DESIGN BACKFITS

PRA techniques have found application in determining the need and nature of design backfits, as well as in assessing the reliability of the modified design. In what follows an example is presented of a reliability assessment and the ensuing benefits.

Case 1

The digital computer control system of one of OHN's generating stations is of such vintage that spare parts cannot be easily procured. A decision is made to replace the computer system hardware by a replacement

design. The computer system has a nuclear safety role in that its malfunction has the potential to cause a loss of reactor power control. Assurance is required that failures of the new hardware will not be any more likely than of the previous design to result in a loss of reactor control.

To obtain the required assurance it was decided to develop a fault tree model for the new system to determine possible ways by which its failures could lead to a loss of reactor control. Particular attention was paid to confirming that the design requirement that safety features built into the previous design be replicated in the new design was met.

The assessment showed that, contrary to expectations, the translation of the old system's defensive mechanisms into the new system, was not implemented reliably. In particular, the ability of the system to monitor its health and place itself in the safe state if a malfunction had occurred had been severely compromised. This capability was implemented in the existing system by means of an analog timing device called the Operations Monitor, which would time out within 5 seconds if it failed to be re-set due to computer malfunction, thereby signalling to reactivity control devices to assume their fail-safe positions. In the new system's equivalent of the Operations Monitor the time out signal was derived from a digital timer which relied on interval timers resident in the computer itself. These interval timers also provided signals for the normal functioning of the computer. Thus, their failure, and failure of devices upstream of them, would not only cause the computer to fail but also prevent the Operations Monitor from timing out. Reactivity control devices could, therefore, be placed in the unsafe state.

Following discovery of the above failure mode, changes were made to the circuit board containing the Operations Monitor such that the Operations Monitor would operate independently of the system's interval timers. This change enabled the system's reliability estimates to be shown to be acceptable.

DISCUSSION

The examples presented above of application of PRA to nuclear power plant operation demonstrate that PRA methods have the potential to provide benefits in a number of areas. Such applications, however, always need to be tempered by a recognition of limitations of PRA, some of which while not necessarily inherent to PRA, nevertheless affect its implementation. For example, if the PRA models are based on out-of-date system design and operational information, its results may be misleading. Also, it needs to be remembered that underlying the PRA models are usually a number of assumptions about plant behaviour. While these assumptions might have been valid at the time the model was developed, their applicability to the situation being assessed must be confirmed. Furthermore, to the extent practical, guidance on actions to take during non-standard configurations should be pre-determined, supported by PRA models as appropriate, rather than established after the configuration has been entered. However, there will always arise unforeseen situations, so on-line use of PRA models is inevitable.

The increased use of PRA in station operation also requires the ability to easily apply the models. This, in turn, places a requirement for efficient and easy-to-use computer tools for solving the PRA models, presenting the information in an easily assimilable form, and interrogating the models. Ontario Hydro expects to implement such tools at its generating stations by virtue of its membership in the EPRI-sponsored and industry-supported Risk & Reliability Workstation development.