Use of Quantitative Indicators of Nuclear Safety in Ontario Hydro

R.T. Popple and S.B. Harvey

Abstract

The measurement of reactor safety performance from a public risk standpoint is rapidly becoming an area of wide interest, both in the public mind and within the industry. This paper outlines the quantified operational risk assessment methodology that has been in use in the Ontario Hydro nuclear-electric program since the early 1960's. It enables an assessment of risk arising from operation to be compared with Ontario Hydro standards and those set by the Federal regulator of the nuclear industry in Canada, the Atomic Energy Control Board. Although the methodology is a main part of the public safety thrust used by Ontario Hydro to achieve acceptable levels of risk, it is not the only part, and other complementary areas are discussed in the paper.

Introduction

Nuclear generation is now the major option for production of electricity in the province of Ontario because hydraulic resources have been developed almost to the economical limit and fossil fuels are expensive.

Ontario Hydro is a publicly-owned Corporation that supplies the electrical needs of the province of Ontario, which contains the industrial heartland of the country and a population of about eight million people. The present Ontario Hydro in-service nuclear capacity is 9,711 MWe, or 9,969 MWee (Table 1).

Public safety is achieved through a defence-in-depth approach to radioactivity containment that allows for occasional operator mistakes and design oversights. Ontario Hydro nuclear-electric stations have 4 overlapping work program thrusts, to protect the barriers to radioactivity release (ceramic fuel, fuel sheathing, heat transport pressure boundary, containment structures, and exclusion zone). These 4 thrusts, which form the basis of its operational safety management program, are:

- ensure that systems which are normally in service (process systems) are reliable;
- ensure that poised safety systems are reliable;
- ensure that equipment and procedural faults are detected, assessed, and promptly corrected, including re-design when necessary; and
- provide in-depth training to operating staff.

The operational safety management program used by Ontario Hydro has been under continuous improvement over the past 25 years as modelling, fault classification, testing, and data manipulation methods have evolved; such development is expected to continue.

The achievement of high levels of public safety and the ability to demonstrate that achievement requires the following:

1 a knowledge of the areas critical to safety;
2 a set of standards or targets which define acceptable performance;
3 a program to monitor performance, respond to problems, and to report the results;
4 an experience review program to establish a) trends, b) the degree of compliance with standards, and c) root causes where performance is unacceptable or deteriorating; and
5 a means of assessing the impact of proposed changes to hardware or operating procedures and of implementing changes consistent with the accepted standards.

Risk Quantification

The key indicator of effectiveness of a public safety management program is quantified risk. It is expressed as the frequency of a postulated event multiplied by its consequence:

$$\text{RISK}_{(\text{EVENT})} = \text{FREQUENCY}_{(\text{EVENT})} \times \text{CONSEQUENCE}_{(\text{EVENT})}. \quad (1)$$

The total risk resulting from station operation is the sum of the events risks

$$\text{RISK}_{(\text{TOTAL})} = \sum_{\text{EVENTS}} \text{RISK}_{(\text{EVENT})} \quad (2)$$

A risk management program could be based on risk from individual postulated events or on total plant risk, or, as is used in Ontario Hydro, both.

Keywords: risk assessment, nuclear safety, public risk, safety systems, safety management, nuclear regulation.

Table 1: Ontario Hydro In-Service CANDU-PHW[2] Nuclear Capacity, 31 December 1986

Station	*Unit*	*Net capacity MWe*	*Net capacity MWee*
NPD NGS	Single	22	22
Pickering NGS-A	1	515	515
	2	515	515
	3	515	515
	4	515	515
Pickering NGS-B	5	516	516
	6	516	516
	7	516	516
	8	516	516
Bruce NGS-A	1	759	770[1]
	2	769	848
	3	759	848
	4	769	848
Bruce NGS-B	5	835	835
	6	837	837
	7	837	837
Total: 5 Stations	16 units	9,711	9,969

In addition to the 9,711 MWe of CANDU-PHW nuclear capacity in service with Ontario Hydro at the end of 1986, a further 4,361 MWe of capacity was under construction.

[1]Incudes electrical equivalent of process steam (only applicable to Bruce NGS-A).

[2]CANadian Deuterium Uranium reactors, heavy-water moderated, use natural uranium fuel, and Pressurized Heavy Water coolant.

The risk to the public from the operation of a nuclear generating station arises from both conventional and radiological hazards resulting from station operation. The conventional risk is not discussed here.

The predominant radiological risk from nuclear station operation results from the potential for premature death due to a radiological dose (measured in rem). The consequence of a given event is therefore measured in rem / event. When this consequence is combined with the expected frequency (events / annum) of the event in question, a measure of risk is obtained.

$$\text{Frequency (events / annum)} \times \text{Consequence (rem / event)} = \text{Risk (rem / annum)}.$$

Risk measured in 'rem / annum' can be directly correlated with a more conventional measure in 'fatalities / annum' (see below, Safety System Unavailability, and Integrated Public Risk).

Systems in a nuclear-electric unit can be broadly separated into process systems and poised safety systems. Process systems are those required to generate electricity; the heat transport systems and reactor power control systems are the most significant from a potential radioactivity release standpoint. Safety systems are poised to shut down the reactor, provide additional fuel cooling if needed, and contain any radioactivity released; they do not play a role in power production.

Ontario Hydro has used the concept of process systems and safety systems in developing its operational risk model. The groups of events which contribute to risk are:

- chronic radiological emissions;
- process system failure with subsequent successful safety system operation (termed single failure);
- process system failure with subsequent failure of a safety system (termed dual failure); and
- process system failure with subsequent failure of more than one safety system (including failures caused by external events).

In Ontario Hydro, separate targets have been developed for chronic and acute risks. Since chronic emissions are directly measurable, a predictive model is not required to enable comparison of results with targets. The Ontario Hydro operational risk management model, therefore, need only consider acute risk. Based on Equation (2):

$$\text{RISK}_{(\text{ACUTE TOTAL})} = \Sigma\,\text{RISK}_{\text{SINGLE FAILURE}} + \Sigma\,\text{RISK}_{\text{DUAL FAILURE}} + \Sigma\,\text{RISK}_{\text{MULTIPLE FAILURE}}. \quad (3)$$

At present, the risk due to multiple failures is not being assessed at operating stations. This is based on a design and licensing requirement that multiple safety system failures should not result from a process system upset; therefore, if any such failure mechanisms are detected, they are eliminated. Design verification activities and an ongoing review of the potential impact of observed faults (locally and world-wide) are intended to eliminate multiple faults. Even if some multiple failure mechanisms remain, their contribution to total risk is expected to be small relative to other terms.

Identification of Critical Safety Areas

The operational risk model described is a means of producing a risk indicator from an existing understanding of overall risk contributors. It is, however, unable to predict actual risk because:

- while it is a design and operating philosophy to maintain independence of safety systems, and of process systems with safety systems, a comprehensive detailed analysis has not been done on operating stations;
- the frequency of process upsets is not based on detailed analysis;
- the analysis of consequences is often highly conservative; and
- the analysis of safety system unavailability assumes, conservatively, that the system provides no benefit.

Ontario Hydro is currently looking at fully integrated event tree / fault tree risk models, i.e., Probabilistic Risk Assessments (PRA) as a means of obtaining a more comprehensive understanding of risk contributors. This improved understanding of risk will be factored

into the operational risk model and is expected to improve its validity and usefulness. Even without a comprehensive PRA, operational experience is expected to yield improvements to our understanding of risk as new events trigger re-assessments.

Ontario Hydro Targets

Ontario Hydro has established targets which, if met, will achieve both the regulatory requirements and the internal public safety risk objective.

Single Failure Frequency

From a public safety perspective the standard for frequency of accidents which have the potential to release radioactive material without safety system action is a maximum of 1 accident per unit in 3 years. Economic considerations would dictate that a target should be much more restrictive than 1 / 3 years.

Safety System Unavailability

Safety system unavailability is defined as the fraction of time that a safety system cannot act as required. An unavailability target of 1×10^{-3} a / a is set to ensure compliance with the regulatory Siting Guide dual accident frequency as follows:

Accident Frequency × Safety System Unavailability ≤ Dual Failure Frequency, (Siting Guide) or

$$\frac{1}{3\,\text{yr}} \times 1 \times 10^{-3} \frac{\text{yr}}{\text{yr}} \leq \frac{1}{3{,}000\,\text{yr}}.$$

The unavailability target is applied to each 'special' safety system individually (i.e., shutdown system; shutdown system no. 2, where installed; emergency coolant injection system; containment system). Targets are also developed for other poised safety-related systems based on the overall importance of the system.

Integrated Public Risk

Ontario Hydro has developed a radiological risk standard based on the principle that:

'The risk to an individual member of the public, from the operation of a nuclear generating station, should be negligible when compared with the everyday risk to which that member of the public is exposed.'

The average risk to the public in Canada for all accidents is approximately 600 premature deaths per annum for every million persons (i.e., 600×10^{-6} fatalities / a). If we define negligible to be less than 1%, the standard would be 6 premature deaths per annum for every million persons (i.e., 6×10^{-6} f / a). Considering a given individual member of the public, his / her risk of death each year would then be 6 chances in one million. The Ontario Hydro standard has been set even more conservatively at 1 chance in a million of a given individual (the most exposed one) suffering a premature death in a one-year period due to releases of radioactive material (i.e., 1×10^{-6} f / a).

This risk standard of 10^{-6} fatalities per annum is converted to a radiological risk standard in rem per annum by using a statistical medical relationship correlating whole-body exposure to a premature death probability:

1 rem whole body = 10^{-4} premature death probability.

Since 1 rem Equivalent Whole-Body (EQWB) dose is defined so as to be equivalent in terms of cancer induction to 1 rem whole-body dose.

1 rem EQWB = 10^{-4} premature death probability.

The Ontario Hydro risk standard can thus be expressed as:

$$\text{Risk Standard} = 10^{-6} \frac{\text{fatalities}}{\text{annum}} \times \frac{1\ \text{rem EQWB}}{10^{-4}\ \text{fatalities}},$$

or Risk Standard = 10^{-2} EQWB dose (rem) / annum

Monitoring, Response, and Reporting

Active Systems

Failures in systems which are directly involved in power production are immediately detectable. A test program is not required. The safety management program focuses on ensuring that, in the short term, operator response to a failure will minimize public risk, and in the longer term, lessons learned from the failure are acted upon.

Short-Term Operator Response

The operator is given guidance regarding the optimum response to a process system failure in the following ways:

- operating procedures specify step-by-step response for events which are anticipated to occur frequently, or where an optimum response can be established with confidence;
- operating procedures specify general response criteria for events which have not otherwise been addressed in detail; and
- operators are trained to recognize and respond to key plant parameters, regardless of the cause of the event.

Reporting

Operators prepare a 'Significant Event Report' (SER) for any serious process system upset. These SERS record the first hand observations of the upset. Based on a subsequent thorough analysis of the event, process system faults are then categorized using the following:

Type A a failure that would have caused significant fuel failures or radiological hazards in the absence of Special Safety System action

Type B a failure which did not require Special Safety System action to prevent significant fuel failures or a radiological hazard, but was due to fortuitous factors

rather than specific design or control provisions

Type C a failure that tended to raise fuel temperature but could not cause significant fuel failures or radiological hazards even in the absence of Special Safety System action

Type D a failure which would have tended to raise fuel temperature in the absence of Special Safety System action if fortuitous factors had been different

Type E a failure that had no effect on fuel temperature, or lowered it

Poised Systems

Poised systems are those which normally monitor process variables and are triggered when an upset occurs (e.g., shutdown system, emergency coolant injection system). A test program is required to detect system failure, and hence to provide confidence that the system would work if needed.

Test Program

It is necessary to determine which functions or components must be tested, and the test frequency. Reliability analysis is used for these purposes.
The system test frequencies are based on:

- the system unavailability target;
- the failure rates of components using either generic or plant-specific data, as available; and
- the degree of difficulty or the risk of spurious operation in doing the test.

For record and analysis purposes, faults of poised systems that are typically detected on the basis of defined testing program, are classified as follows:

A *Type 1* fault significantly reduced the effectiveness of the system, such that it would have been of little or no benefit if the worst possible process system failure had occurred.
A *Type 2* fault reduced the effectiveness of the system, such that it would have failed to satisfy the design intent. However, the system would still have operated and significant benefit would have been gained from its operation.
A *Type 3* fault reduced the level of redundancy that is built into the system. The effectiveness of the system was not significantly reduced and the design intent could still be satisfied.
A *Type 4* fault reduced the effectiveness of the system, or a single component, such that it was outside normal operating limits. However, the design intent could still be satisfied.
A *Type 5* fault had no negative effect on the system.

Type 4 and 5 faults are maintained in the data base to ensure auditability of the classifications (eg, a Type 4 which should be a Type 3) and to allow reclassification if design changes are considered.

Special Safety System Reporting Indices

Conversion of observed system performance into unavailability estimates can be done in many ways. Ontario Hydro uses 4 indices because no single index can provide total insight into system performance given the statistical limitations of finite data. These indices are:

1 *system inoperability*
2 *observed system unavailability*
3 *derived system unavailability*
4 *expected system unavailability*

System Inoperability

System inoperability is the fraction of time during the past year that a system is fully incapable of providing protection for the events with which it is designed to cope. This index is determined directly from observation. It does not include marginal failures to meet the design intent of the system, and is therefore a non-conservative measure of system performance. However, when used in conjunction with *observed system unavailability* (see below), it is useful in distinguishing between major system faults, which definitely impact on public risk, and faults which may, in reality, represent only an erosion of the conservative assumptions used in the plant safety analysis.

Observed System Unavailability

(Also known as *actual past unavailability*)
Observed system unavailability is the time fraction that the overall system was known to be *not fully available* during the past year. Again, this index is determined directly by observation. This index includes any faults which result in *system inoperability* with all other faults (or combination of faults) which resulted in the system not being capable of fully meeting the design intent. Hence, it is a conservative measure of system performance. While this index provides a conservative measure of the actual system performance, it is susceptible to large statistical fluctuations from year to year, which makes decision making difficult if based on this parameter alone. It also provides little information on component or subsystem performance.

Derived System Unavailability

(Also known as *derived past unavailability*)
Derived system unavailability is a calculated index which uses a reliability model (generally a simple functional block model) to combine the results of the testing program obtained over a 1-year period. All unsafe faults which occurred over the past year are included, and subsystem / component unavailabilities are calculated using an estimate of average future fault durations. This index is sensitive to short-term changes in system performance, and provides more information than *observed system unavailability* on the contribution of individual component / subsystem failures to overall system performance. It also provides an indication of the statistical significance of the value of the *observed system unavailability* in a particular year. If *observed*

Table 2: Summary of Risk Indicators vs Experience

		*Average observed lifetime performance***			
	Target	*PNGS-A*	*PNGS-B*	*BNGS-A*	*BNGS-B*
Unit years in-service		55	5	32	2
Single failure rate	1 / 3 f / a	0.2	0	0	0
Shutdown system 1					
Unavailability*	1 a / a***	0.27	0	0.97	0
Inoperability*		0.017	0	0	0
Shutdown system 2					
Unavailability*	1 a / a	N / A	0.007	2.15	0.009
Inoperability*		N / A	0	0	0
Emergency coolant injection system					
Unavailability*	1 a / a***	89.0	0.04	30.5	1.19
Inoperability*		1.0	0.04	0.003	0
Containment system					
Unavailability*	1 a / a***	30	0.07	1.97	0.83
Inoperability*		0	0	0	0
Acute risk indicator	10^{-2} rem (EQWB) / a	2.4×10^{-3}		1.6×10^{-3}	1.6×10^{-4}

*All unavailability and inoperability targets / results are to be multiplied by 10^{-3}.
**Calculated from in-service date to end 1985.
***Target is 3×10^{-3} for Pickering A.

system unavailability is significantly higher than *derived system unavailability*, this indicates that faults on redundant components overlapped to a greater extent than expected, or that fault durations were much longer than we would reasonably expect in the future. Conversely, if *observed unavailability* is much less than *derived*, this can be taken to indicate a fortuitous situation which should not be expected to continue in the long term.

Expected System Unavailability
(Also known as *predicted future unavailability*)
Expected system unavailability is a calculated index which uses the same reliability model as *derived system unavailability* to combine all relevant subsystem (or component) experience obtained to date on the system of interest. Where few or no failures have been observed, a 50% confidence chi-squared estimate of failure rate is used to provide an estimate of subsystem (or component) performance. After a few years, this index provides a statistically valid upper limit estimate of long-term average system performance. As it uses all relevant experience, it does eventually become relatively insensitive to sudden changes in the performance of equipment, but such changes are detected by other means (e.g., *derived system unavailability*).
There is one point which should be emphasized in looking at actual experience: although the second, third and fourth indices contain the word 'unavailability,' this does *not* denote the time that the system is totally incapable. They quantify the effects of faults which reduce the redundancy or capability of the system, even though the system may still provide adequate protection for most events. These parameters are, in reality, conservatively defined indices which combine experience in a predetermined manner. The achievement of target using these indices indicates excellent system performance; but because of the conservatism inherent in this approach, failure to meet target does not necessarily imply unacceptable risk.

Results of the Safety Management Program
Table 2 shows the lifetime average of the key risk management indices as compared to their targets for a spectrum of mature and immature in-service stations as of end of 1985. Table 2 is intended to be illustrative only. In any given year, or on a particular system, targets may be exceeded, but the overall risk indicator has always been achieved by a considerable margin. Design or operational changes have been made, or are being made, in all cases where a system target is consistently not met. The operational risk indices have shown where such changes are needed.

The following summarizes Ontario Hydro's experience to the end of 1985:

1 There has not been a failure which resulted in a release of radioactivity causing a measurable radioactivity dose to a member of the public in over 100 reactor-years of in-service operation.

The failure rate of process systems exceeded target at Pickering NGS-A in the initial years of station operation, but design changes were successful in reducing the failure rate to well below target.

System unavailability and inoperability targets have generally been met, in many cases with wide margins. Although the overall risk from Pickering operations is

significantly better than target (40 times), the Pickering emergency coolant injection system performance has been well above target (30 times), warrants reliability improvement, and design changes are in progress. Similarly, design changes have been made to improve the unavailability of the Bruce-A emergency coolant injection system.

The Pickering NGS-A containment system average performance is well over target. The vast majority of this unavailability is due to a single penetration which had degraded and remained undetected for over 1 year. A comprehensive test program has been instituted to avoid a recurrence and there have been no similar undetected holes in containment either at Pickering or at other stations, which benefitted from a knowledge of the failure mode. No design changes were warranted.

All of the Pickering experience has been incorporated in the design and operating practices of subsequent stations; this is reflected in the observed good performance of these stations and in our expectation of good future performance at Pickering NGS-A.

2 A quantitative and systematic operational safety management program can demonstrate achievement of acceptable public safety while allowing for design, equipment, and operator failures. It can further provide a prioritization of unavailability contributors that can be systematically attacked and eliminated where justifiable.

3 The approach is effective but not perfect and is undergoing continuous improvement.

4 Past achievement cannot justify complacency, and a continued program of vigilance and improvement is in place.