OPTIMIZATION OF THE OPERATING ENVELOPE AND SAFETY MARGINS USING PRA METHODS

Cristian Stoica
Cernavoda Nuclear Power Plant
Cernavoda, Romania

C. Keith Scott
Atlantic Nuclear Services Ltd.
Fredericton, New Brunswick

Paper presented at the CNS Nuclear Simulation Symposium, Niagara-on-the-Lake, Ontario, September 7-9, 1997.

OPTIMIZATION OF THE OPERATING ENVELOPE AND SAFETY MARGINS USING PRA METHODS

Cristian Stoica
Cernavoda Nuclear Power Plant
Cernavoda, Romania

C. Keith Scott
Atlantic Nuclear Services Ltd.
P.O. Box 1268, Fredericton, N.B. E3B 5C8

A major challenge in the operation of a nuclear power plant is the maintenance of an acceptable level of risk when equipment performance degrades through component failure or system ageing. The special safety systems play a particularly significant role in this regard. They are routinely tested to demonstrate compliance with availability requirements. The minimum allowable performance capability of systems is derived from safety analysis and other simulations of system performance and response to abnormal events. Overall station performance and risk management can be improved by linking the analyzed operating envelope with the operational performance of systems. The purpose of this paper is to report on investigations of the use of PRA methodology to optimize the operating envelope and safety margins using "live" plant data.

1. INTRODUCTION

A nuclear plant is licensed on the basis of safety assessments of the risk to the public from its operation. This 'known' level of risk is determined on the basis of the plant design. However, it is a licence requirement that the level of risk be known and maintained throughout the life of the plant. This requirement is challenged by the ageing and replacement of equipment.

PRA methods offer one tool for providing a systematic and rational approach to defining operating limits. In this paper we report on an initial investigation of an operations model that is risk based. As such, it offers the potential to give guidance on the risk throughout the operating history of the plant.

In Section 2, a fairly generic operating model for management of system performance is described. This model is then used to construct a probabilistic risk model as described in Section 3.

2. IMPAIRMENTS OF SYSTEM PERFORMANCE

Operating staff have procedures for addressing system impairments that degrade the performance of the plant. Where there is an incremental risk to the public the procedures give corrective actions to reduce the risk to an acceptable level. One approach for developing procedures is to classify impairments according to their significance based on the incremental risk.

The primary criteria for classifying impairments is their 'operational significance' rather than their 'actual significance'. Figure 1 illustrates the operational limits (boundaries) and impairment regimes (bands).

The following three cases illustrate the philosophy and significance of the impairment classifications.

Level 3

The boundary between the normal operating range and Level 3 impairments is the point at which Operations will raise a WORD to restore the system to its intended operating state.

The system is said to be impaired because action is taken to return it to the intended operating state. There may be a decrease in public safety when the boundary is crossed. However, the boundary is determined primarily by operational considerations.

Consider the trip logic for a shutdown system (SDS) as an example of the Level 3 impairment. If a channel is tripped, it is in the safe state until there is a need to perform a test to confirm the availability of the system. Because there is a requirement to return the system to the normal or poised state from the safe state it is considered impaired.

This case is classified a Level 3 impairment, the lowest level, because the maintenance work does not need to be prompt (i.e., within hours).

Level 2

The transition to a Level 2 impairment is the point at which prompt action is required to place the system in a safer state by returning it to the normal operating range or reducing the severity of the impairment to Level 3.

The prompt action is required because there is potentially a significant increase in the risk to the public. That is, the risk could be significantly different than assessed for normal operation. In keeping with the Reactor Operating Licence,

prudent operation dictates action to remove the incremental risk.

An example of a Level 2 impairment is the unsafe failure of a trip channel on an SDS leaving the initiating logic dependent on each of the other two channels operating as intended. In this configuration the SDS has a substantially lower availability than assumed in the safety assessments supporting the Reactor Operating Licence.

The impairment can be reduced to a Level 3 impairment by tripping the channel with the fault.

Level 1

The system has a Level 1 impairment whenever it is outside the licensed envelope for operation. Prompt action is required to bring the system back within the licensed envelope and a safe state.

The impairment is considered very significant because it is a licence violation. The safety significance of a Level 1 impairment depends upon how far the licence limit is from the safety limit.

An example of a Level 1 impairment would be two trip channels of an SDS having unsafe faults. That is, the performance of the channels would be outside the licensed envelope. An immediate shutdown is required as the response for a Level 1 impairment.

Operating Limits and Safety Margin

The operating limits that define the thresholds for the different impairment levels are taken from licence conditions, the OP&P, operating manuals and test procedures.

In a systematic approach these operating limits should be based on the incremental and absolute risk to the public.

With reference to Figure 1, the boundary of the Normal Operating Range is the Operating Limit. The Safety Limit must be beyond the operating envelope. For this dismission the safety limit is assumed to be identical to the Licence Limit.

The Safety Margin is the extent to which the Safety Limit exceeds the Operating Limit. The safety margin can be degraded by changes in both the safety limit and the operating limit due to equipment changes and ageing of the plant.

During the life cycle of the plant the safety margin must be maintained sufficiently large that the public risk objectives are assured.

3. DETECTION OF IMPAIRMENTS

From the operations model for management of system performance as described in Section 2, we can construct a probabilistic model to optimize the safety margin and to minimize the risk. This model is shown in Figures 2, 3, and 4.

Because of the uncertainty in test results, we must make allowance for those results which indicate the system is in a safer state than it actually is. There are then three test results of concern:

(a) the test indicates the system is in the operating range when it is unavailable;

(b) the test indicates the system is within the operating range when it is within the safety margin; and

(c) the test indicates the system is within the safety margin when it is unavailable.

We do not consider result (c) in the model because operator action is being taken to correct the result. Its significance depends upon the response time mandated for that level of impairment. The other two results are combined for optimization below.

The undetected unavailability for one failure is:

$$A = \sum_{k=1}^{N} P_f^{\,k} \times (k \times \Delta t + t_a) = \Delta t \times \sum_{k=1}^{N} k \times P_f^{\,k} + t_a \times \sum_{k=1}^{N} P_f^{\,k} = \Delta t \times \left(\sum_{k=1}^{N} k \times P_f^{\,k} + a \times \sum_{k=1}^{N} P_f^{\,k} \right)$$

The unavailability due to the unnecessary maintenance:

$$B = \int_{av.dom.} P(x \in av.dom. \rightarrow sm.dom.)\,dx \times t_b = \Delta t \times b \times$$

$$\int_{av.dom.} P(x \in av.dom. \rightarrow sm.dom.)\,dx$$

From a safety point of view (to ensure the accuracy of reliability analysis) the sum of these two terms should be much smaller than the predicted unavailability:

$$\lambda \times A + B \ll \Lambda \times \left(\frac{\Delta t}{2} + t_r \right)$$

From an operating point of view we should minimize the sum $\lambda \times A + B$.

The following is a numeric estimate for the terms A and B.

Term A

It is not necessary to demonstrate the convergence of the series that appear in A because during the plant life only a finite number of tests will be performed. Assuming that the equipment is tested weekly for 30 years the number of tests is 1560. Assuming a 50 percent probability the undetected failure will be discovered on the next test, the contribution of the last 1510 terms of each sum is negligible. As a consequence we can estimate A using only 50 terms. Assuming $a = 1$ (i.e. the equipment will not be repaired until the next scheduled test) the value of A decreases from $3\Delta t$ in case of zero safety margin to $0.052\Delta t$ for a 2σ safety margin.

Term B

The integrated convolution represents a part of the distribution of the test results. It can be approximated by the fraction of tests that indicate a performance inside the safety margin. To find a reasonable way to normalize this convolution we should consider the situation around the safety limit. There is a probability that if the equipment performance is inside the safety limit the test result will be in the unsafe region and the equipment will be declared unavailable. Also, there is a probability that if the equipment performance is in the unsafe region the test result will be in the safe region and the equipment will be declared available. Because we have no reason to believe that at the safety limit the distribution of possible equipment performance has a discontinuity and we expect the probability of equipment performance to be around the safety limit we can use the following assumption:

The probability that a failed state will be detected as a "not failed" state by the test is equal to the probability that the an unfailed equipment state will be detected as a "failed" state at the test.

This assumption is not correct but we expect that the error will be small due to the low probability that the equipment performance is around the safety limit. Using

this assumption we can normalize the distribution of test results with the value inside the "available" domain to (1-Λ).

$$\int_{av.dom.} P(x \in av.dom. \neg av.dom)dx = 1 - \Lambda$$

Having the numerical values for A and B, the optimization problem of the safety margin can be evaluated.

4. SUMMARY AND CONCLUSION

We have begun a program to introduce probabilistic risk assessment into the management of the operating operational performance of safety related systems. An approach such as this is needed for risk based guidance in modifying the operating envelope as equipment ages or is replaced. Ultimately, it would form the link between a live PRA model for the plant and the operating procedures for managing system performance.

In this initial phase of the study, we have used an operational model that is common in the industry. From this it is possible to construct a probabilistic model of the safety margin that can be optimized. Further consideration needs to be given to the dependence upon the response time for Level 3 impairments and the selection of a threshold for Level 2 impairments.

5. NOTATIONS IN TEXT

Notations:

Δt	-	time interval between tests
t_r	-	restoration time after the equipment is found unavailable (includes both access time and repair time)
P_f	-	the probability that the real value of the measured parameter is in the unsafe region but the measurement result is in the operating region
Λ	-	the total probability of equipment failure (includes all failure modes)
λ	-	the probability of equipment failures that result in a continuous degradation of equipment performance (it is part of Λ)
t_a	-	the time between the test with the result

		inside the safety margin and the subsequent equipment performance restoration (it should be at least equal to t_r)
t_b	-	the equipment repair time from the moment the equipment is isolated until it is made available
a	-	the relative measure of t_a (i.e.$t_a/\Delta t$)
b	-	the relative measure of t_b (i.e.$t_b/\Delta t$)
r	-	the relative measure of t_r (i.e.$t_r/\Delta t$)
$\int_{av.dom} P(x \in av.dom.\rightarrow av.dom.)dx$		the probability that the status of available equipment will be measured as being inside the operating region or safety margin
$\int_{av.dom} P(x\epsilon\ av.dom.\rightarrow sm.dom)dx$	-	the probability that the status of available equipment will be measured as being inside the safety margin.

Acknowledgement

The work reported in this paper was done as part of an IAEA sponsored training program. C. Stoica received an IAEA Fellowship for training at Atlantic Nuclear Services Ltd.

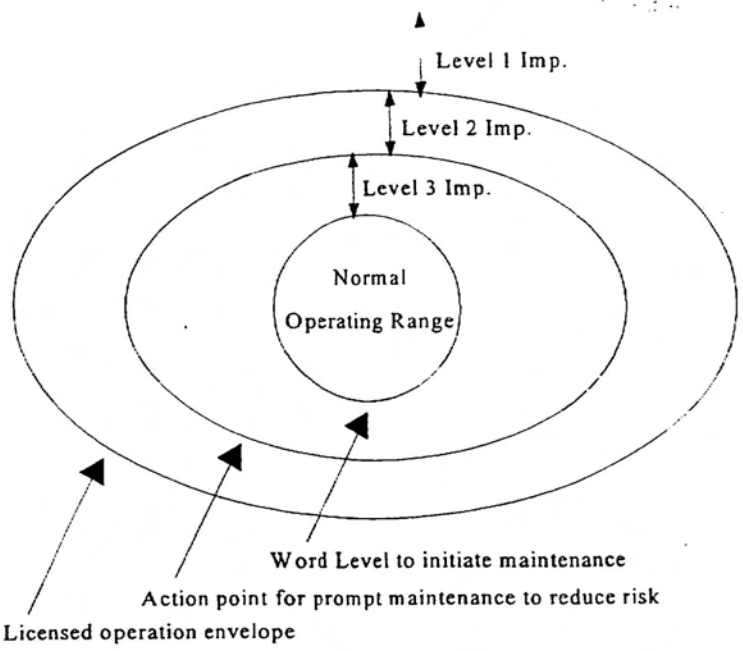

Figure 1 - Illustration of Impairment Levels and Their Operational Significance

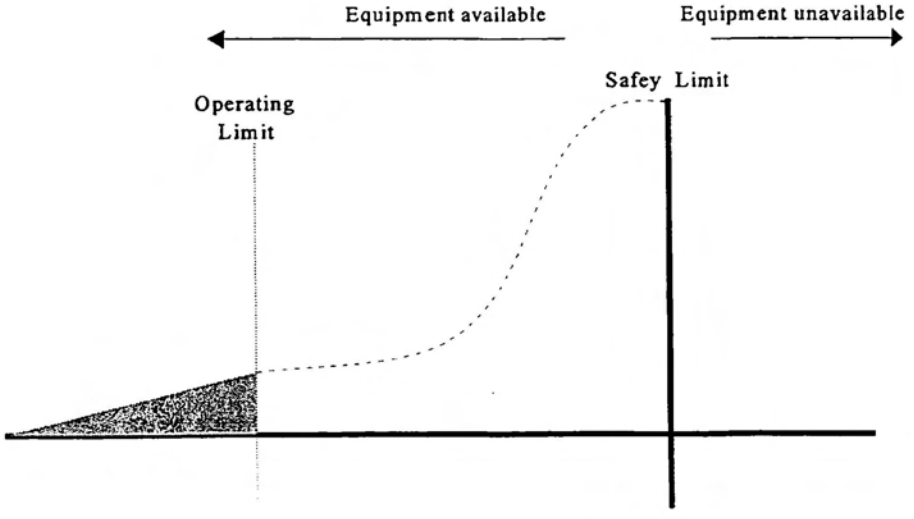

Figure 2 - Domain of Failures Undetected by Testing

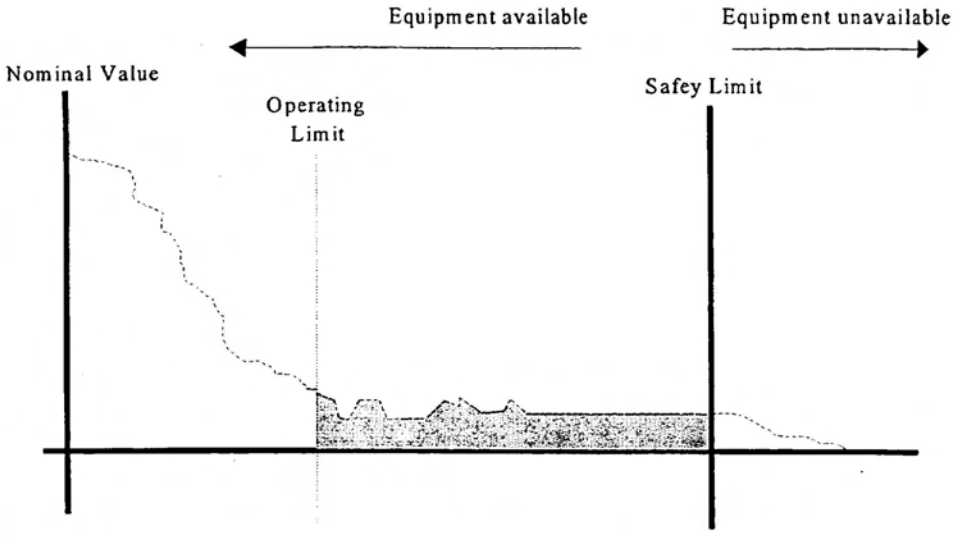

Figure 3 - Domain of Equipment Unavailability Due to Unnecessary Maintenance

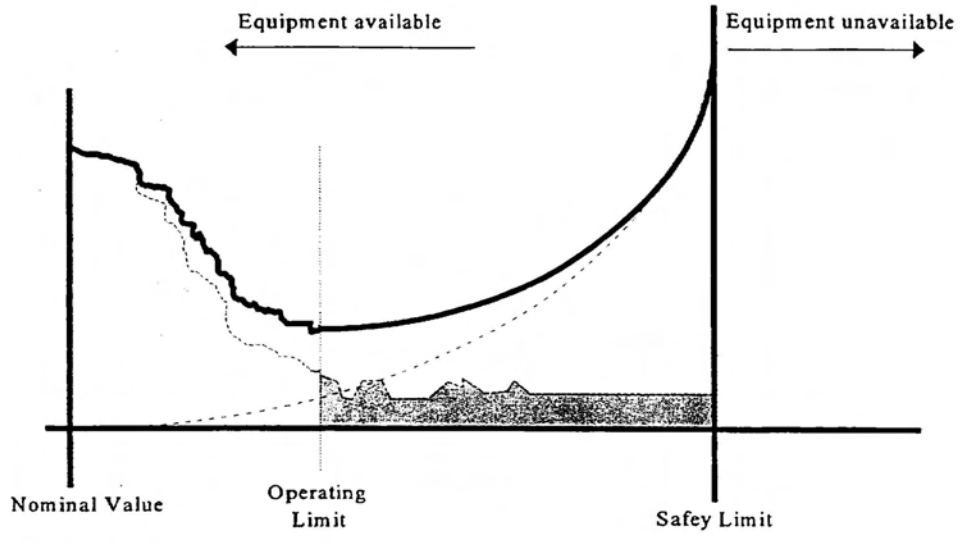

Figure 4 - Optimization of Safety Margin