A RISK-BASED EVALUATION OF ACTION REQUIREMENTS
FOR FAILURES IN SYSTEMS REQUIRED FOR SHUTDOWN*

T. Mankamo
Avaplan Oy, Finland

I. Kim and P. Samanta**
Brookhaven National Laboratory

INTRODUCTION

When the systems needed for the safe shutdown of a nuclear power plant are inoperable or degraded, the risk of shutting down the plant may be comparable or even higher than that of continuing power operation with the equipment inoperable but giving priority to repairs. This concern arises because the plant may not have sufficient capability for removing decay heat during the shutdown. However, in many cases, plant Technical Specifications (TSs) require "immediate" plant shutdown. In this paper, we present risk-based analyses of the various operational policy alternatives available in such situations. These analyses can be used to define risk-effective requirements for those standby safety systems under discussion. We applied the method to multiple failures in residual heat removal (RHR) and standby service water (SSW) systems of a boiling-water reactor (BWR) nuclear plant.¹

This paper has several objectives: (1) to summarize the methodology for evaluating the risk impact of limited conditions for operation (LCOs) requiring plant shutdown, explicitly considering the shutdown risk; (2) to present the results of its application to the RHR and SSW systems of a BWR; (3) to describe the results of sensitivity analyses to evaluate additional operational options, such as imposing explicit testing requirements for redundant trains; and (4) to provide insights on practical guidelines to improve the LCOs and associated allowed-outage times (AOTs) for the systems.

METHODOLOGY

The risk impacts of the basic operational alternatives were evaluated by first modeling phased missions for shutdown cooling in terms of extended event-sequence diagrams (EESDs) with embedded state submodels. The EESDs were then quantified with an explicit consideration of the dynamic and transitional aspects of shutdown operation, including stochastic repair-time distribution of failed components and the heatup time of the suppression pool. The development of EESDs as a new sequence-modeling tool evolved from the recognition of the need for realistic, time-dependent risk quantification, as encountered in the modeling of shutdown-related transients and consideration of operational alternatives in

*Work performed under the auspices of the U.S. Nuclear Regulatory Commission.

**To whom the correspondence should be addressed at Brookhaven National Laboratory, Building 130, Upton, New York 11973.

Received by OSTI

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED JUL 21 1992

failure situations of standby safety systems. This methodology builds on earlier work by Mankamo et al.² to address multiple failures for a BWR plant in Finland.

To develop guidance for an operational policy where the risk impact is controlled as far as possible, various operational alternatives are defined and evaluated. Sensitivity analyses also are performed to assure robustness of final decisions with respect to data uncertainties and modeling assumptions.

APPLICATION

The risk-based evaluation is based on comparing "AOT operating risk" (i.e., the risk associated with continuing power operation with the equipment inoperable) during repair time versus "AOT shutdown risk" (i.e., the risk associated with shutting down the plant with the equipment inoperable). Figures 1 and 2 show typical results from risk quantification that are useful in evaluating the operational alternatives, and thereby, the AOTs and LCOs of technical specifications. Figure 1 depicts the AOT risk impacts in terms of core-damage frequency for both alternatives in various failures of the SSW system. Figure 2 shows the cumulative AOT operating and shutdown risks versus repair time in various failures of the SSW system. In double failures, i.e., where two SSW trains are detected failed during power operation, the AOT operating risk is smaller than the AOT shutdown risk until the repair time of 3 days. Hence, we may conclude, from a quantitative risk point of view, that it is more beneficial to continue power operation than to shut down the plant if the component's operability can be restored within 3 days following the failure detection. Where the repair takes longer than 3 days, it is advisable to shut down the plant. However, we also should take into account other considerations, such as uncertainties in the risk evaluations, the timing of shutdown, and the testing of redundant trains.

SUMMARY OF RESULTS

The standby safety systems needed for safe shutdown, such as the RHR and SSW systems, require different considerations from other systems in evaluating the potential improvement to their LCO requirements (including AOTs and action statements). Existing LCO requirements for these systems call for short time for repair, and sometimes immediate shutdown as more failures are observed. However, as opposed to other safety systems that are not required for shutdown, failures in these systems often result in a large shutdown risk that may be higher than the risk of continued operation. The TS action statements for these situations need to reconcile these risk implications.

Realizing that the risk for both alternatives is significant, the action requirements should be directed to minimizing the risk. What should be avoided is situations where the AOT operating risk is incurred by attempting to repair the failed equipment and then proceeding to shutdown because of the inability to complete the repair within the allowed downtime, thus incurring risk both from continued operation and from transition to shutdown.

We found, not surprisingly, that the risks for multiple failures are significant. However, there is no clear requirement in TS to identify multiple

failures. Even with the TS surveillance requirements, it is conceivable that such situations may remain undetected.

Caution is needed in devising TS action requirements for failures in the systems needed for shutdown. Comparison of the operational alternatives should not be the only factor in defining the action statements. If followed, this approach would result in longer AOTs for multiple failures, thus providing incentives to declare multiple failures when repairs for a single failure cannot be completed within the prescribed AOT.

The results presented here are based on a plant-specific application carried out for the RHR and SSW systems of a BWR. However, similar situations may exist for several other systems; namely, emergency power (EP) system in a BWR, and auxiliary feedwater (AFW), service water (SW), component cooling water (CCW), RHR, and EP systems in a PWR.

REFERENCES

1. T. Mankamo, I.S. Kim, and P.K. Samanta, "Risk-Based Improvement of Technical Specification Action Statements Requiring Shutdown: Pilot Application to the RHR/SSW Systems of a BWR," Brookhaven National Laboratory, Draft Report, April 1992.
2. T. Mankamo and M. Kosonen, "Continued Plant Operation Versus Shutdown in Failure Situations of Standby Safety Systems," IAEA/Tech Spec Pilot Study Program, NKS/SIK-1(91)4, August 1991.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Figure 1. Instantaneous AOT core-damage frequency (f_{CoreD}) for continued operation (CO) and shutdown (SD) alternatives in failures of the SSW system (For example, 2:CO denotes the CO alternative in the failure situation of two SSW trains being inoperable.)

Figure 2. Cumulative AOT core-damage risk versus repair time in failures of the SSW system (For example, 2:CO denotes the CO alternative in the failure situation of two SSW trains being inoperable.)

END

**DATE
FILMED**

12 / 15 / 92