CONF-9209300--1

BNL-NUREG-48150

Risk-Based Evaluation of Allowed Outage Times (AOTs) Considering Risk of Shutdown*

T. Mankamo
Avaplan Oy, Finland

I.S. Kim and P.K. Samanta
Brookhaven National Laboratory, USA

BNL-NUREG--48150

DE93 005589

Abstract

When safety systems fail during power operation, Technical Specifications (TS) usually limit the repair within Allowed Outage Time (AOT). If the repair cannot be completed within the AOT, or no AOT is allowed, the plant is required to be shut down for the repair. However, if the capability to remove decay heat is degraded, shutting down the plant with the need to operate the affected decay-heat removal systems may impose a substantial risk compared to continued power operation over a usual repair time. Thus, defining a proper AOT in such situations can be considered as a risk-comparison between the repair in full power state with a temporarily increased level of risk, and the alternative of shutting down the plant for the repair in zero power state with a specific associated risk.

The methodology of the risk-comparison approach, with a due consideration of the shutdown risk, has been further developed and applied to the AOT considerations of residual heat removal and standby service water systems of a boiling water reactor (BWR) plant. Based on the completed work, several improvements to the TS requirements for the systems studied can be suggested.

DISCLAIMER

*Work performed under the auspices of the U.S. Nuclear Regulatory Commission (USNRC). The views expressed are those by the authors and do not necessarily reflect any position or policy of the USNRC.

1. INTRODUCTION

1.1. Problem Formulation

Defining the Allowed Outage Time (AOT) will be considered here as a risk comparison between two alternatives:

CO: Continued operation: repairs undertaken at an increased risk level, while in the full power operation state

SD: Decided shutdown: a controlled shutdown undertaken to make repairs in a zero power state (usually, a cold shutdown state)

The SD alternative includes a specific risk constituted by possible disturbance transients during power reduction and cooldown. Furthermore, if the initial failures affect the residual heat removal (RHR) function, the need to operate the degraded RHR systems may impose a substantial risk. These risks cannot be readily determined but require a closer evaluation. The operational decision alternatives, and relevant operational flow branches for an AOT case, are illustrated in Figure 1. The risk implications of these operational alternatives are discussed in more detail in Section 2, along with highlighting the characteristics of the approach as compared with more conventional, risk-based AOT considerations.

The uses of this kind of analysis are to:

- identify noncoherent requirements in Technical Specifications (TS) that may result in increased risk as opposed to alternative, safer options,
- alert plant personnel about situations where quick diagnosis and resolution of the problem is important, and
- provide a basis for risk-effective, practicable action statements to minimize the risk impact of operational events.

1.2. Background and Scope

The methodology is built on the recent work and applications for the residual heat removal (RHR) and standby service water (SSW) systems of a BWR plant in the United States [1], and on the earlier work for a boiling water reactor (BWR) plant in Finland [2,3]. The basic development and criteria for risk-based AOTs are more completely presented in References [4,5].

This paper will describe key features of the risk comparison approach, supplementing earlier publications. Especially, the addition to long-term risk from a preset AOT will be considered. The completed work and practical applications thus far have resulted in several suggestions to improve the TS action statements. These insights also are discussed.

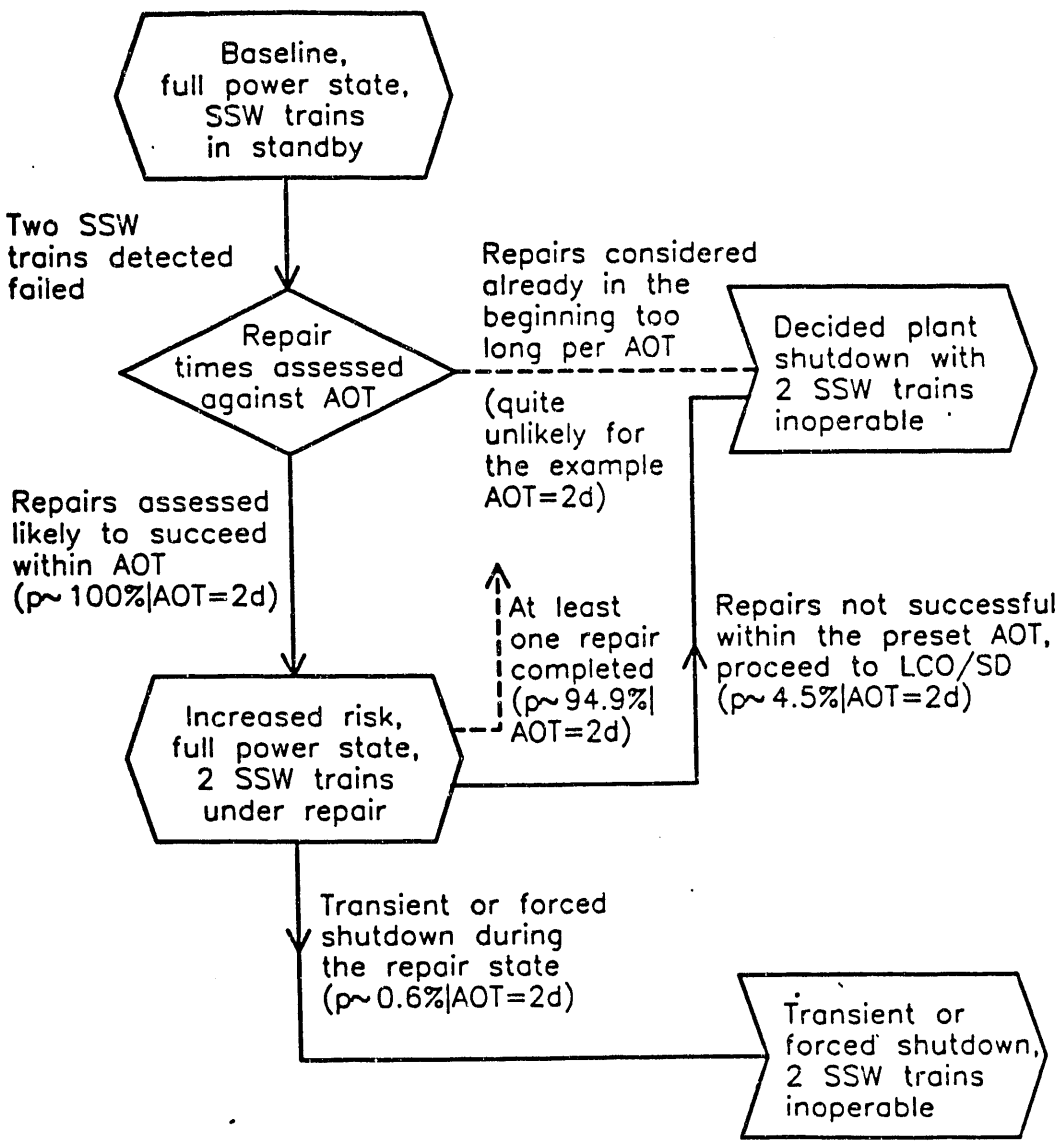

Figure 1. Operational states and flow paths in a failure situation of a standby safety system. The likelihood of the branches is illustrated here by data relevant for SSW train failures in a BWR plant [1].

2. RISK COMPARISON APPROACH

The method and approach are illustrated by using the results from a recent pilot application to failures of three redundant SSW trains [1]. These trains constitute a part of normal RHR path, but also serve as a vital component-cooling function in most front-line safety systems, and in jacket cooling of diesel generators.

2.1. Basic Operational Alternatives

Consider a failure situation covered by an AOT, and the relevant operational states and flow branches, as presented in Figure 1. Instantly when failure is detected, the increased risk level in the full-power state is entered. There are three principal exits:

coA Repairs or some other type of restoration is successful within the AOT. In cases of multiple failure, the completion of one repair usually significantly reduces the situation-specific risk, and thereby, transfers to another, safer state (not shown explicitly in Figure 1).

coB A random transient or some critical cause forces plant shutdown during the full-power repair state.

sd A controlled plant shutdown is undertaken because the repairs are not successful within the AOT.

The likelihood of exit path *coB* is usually small, because the probability of the transients and forced shutdown needs is low over the normal mean repair time.

The likelihood of exit path *sd* is determined by the distribution of repair time against the AOT.

If no AOT is given, then the operators will promptly proceed from detecting the failure to a controlled plant shutdown. In this case, the expected risk is constituted merely by the *sd* branch, neglecting the short-duration risk while at power before the transition to shutdown. This is the principal SD alternative defined in Section 1.1.

If an AOT is given, the expected risk per failure situation includes the net contribution from all the three possible branches, weighted according to their likelihood. Assuming infinite AOT, or in practice, a long AOT compared with the mean repair time, this risk corresponds with the principal CO alternative defined in Section 1.1. (The influence of AOT in relation to mean repair time is discussed later.)

In a "conventional" AOT consideration, plant shutdown risk is assumed negligible in comparison with the temporarily increased risk level, and cumulated risk over a repair time. This may be a reasonable assumption for the failure cases of some specific systems, but not necessarily for the RHR or SSW systems, especially needed in the plant shutdown states, as shown by the results from recent studies [1-3].

2.2. Risk Measures for Comparing Operational Alternatives

In SD/CO risk comparisons, the primary risk variables to be considered in setting AOTs are the instantaneous risk frequency in the failure situation, and the cumulating risk over a predicted repair time (also a situation-specific risk). These are illustrated in Figure 2 by using SSW case data [1]. In addition,

the incremental influence by a preset AOT in the long-term risk average is of interest, and will be discussed here.

2.2.1. Instantaneous Risk Frequency

The instantaneous risk frequency, i.e. the probability of undesired end event per unit of time (here, core-damage frequency as defined in Level 1 PSA analysis) is shown in Figure 2a for both CO and SD alternatives, over a multiplicity of failure situations of three redundant SSW trains [1]. The main interest focuses on whether a lower risk level will be reached after plant shutdown, because this is a precondition of the SD alternative being viable at all. There may be extreme cases, where the risk frequency would be higher in the zero-power state as opposed to full-power state, for example, in a total failure of the standby RHR systems of a BWR plant, where the normal power conversion system/turbine condenser is unstable when used at low steam rates.

2.2.2. Cumulating Risk Over Predicted Repair Time

Figure 2.b shows the cumulating risk over the predicted repair time, i.e. the integral of risk frequency over a given repair time, for both CO and SD alternatives, over a multiplicity of failure situations of three redundant SSW trains [1]. The main interest in these curves is: at what time do the SD/CO alternatives cross? The SD alternative is appropriate for longer repairs than the threshold value. Therefore, the cumulating risk is important in determining a proper AOT in the SD/CO comparison.

Generally, the AOT should be comparable with the crossing point of the cumulating risk over predicted repair time. In practice, when the SD/CO curves are close to each other, the crossing point need not be followed strictly, especially when taking into account the uncertainties of the risk calculations (to be discussed later; compare with Figure 5). Practical and operational reasons may motivate the use of limited, discrete values for AOTs such as 1, 3, 7, 14, or 30 days.

2.2.3. On the Concept of "Baseline" State and Risk

The baseline risk (Figure 2a) will be used here to refer to the risk level when the safety systems are in their nominal state. For most safety systems, this means the standby state without any components known to be inoperable. The latent failures of these components are only detected by surveillance tests, or in demand situations. Their likelihood is the prime ingredient of the baseline risk. For some safety systems or components, the nominal state may also be operating state. Consequently, failures of those components are usually directly revealed by instrumentation or process symptoms. If an initiating event occurs during the baseline state, the instantaneous unavailability is initially zero for these systems, but they may fail during the mission period, and, in that way, also contribute to the baseline risk.

Disconnection for testing or maintenance, and detection of critical faults in surveillance testing of standby components, or failure to run of operating components, are deviations from the baseline state.

When considering AOT situations for a safety system, it is important to carefully exclude from the baseline state all unavailability states of safety-system components, which would interfere with the LCO rules for the considered systems. Such interfering combinations should be considered explicitly as distinct AOT situations, and not included implicitly as is normally done in PRA studies for repair and maintenance downtimes.

The long-term risk is composed of the average baseline risk plus the expected value of the increments due to deviations from the baseline. In practice, this is too tedious a way of obtaining the total average risk level, and the standard PRA approach is considered appropriate for that purpose.

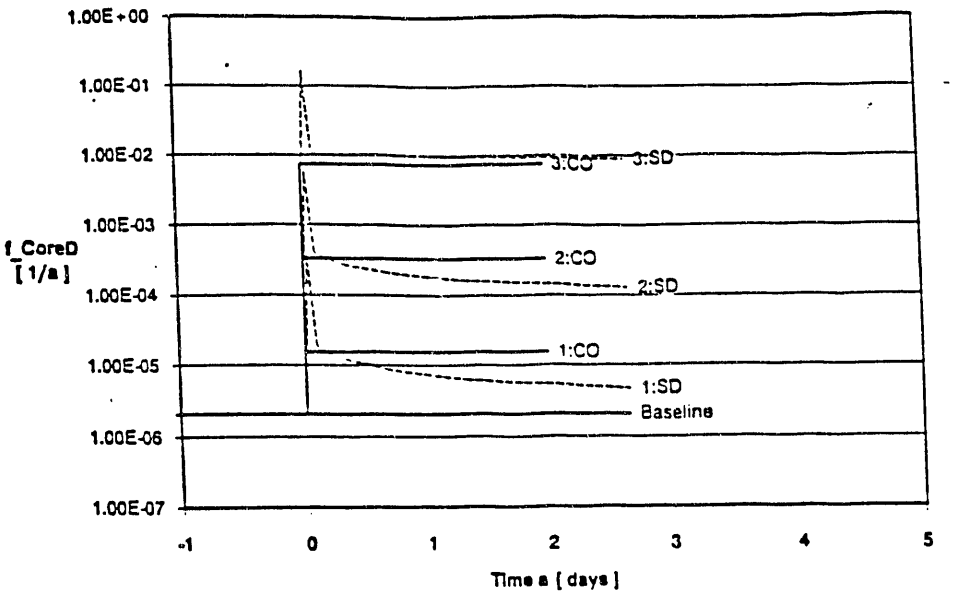

Figure 2a. Instantaneous risk frequency for the continued operation (CO) and plant shutdown (SD) alternatives in failures of SSW trains. For example, 2:CO denotes the continued operation alternative when two SSW trains are inoperable [1].

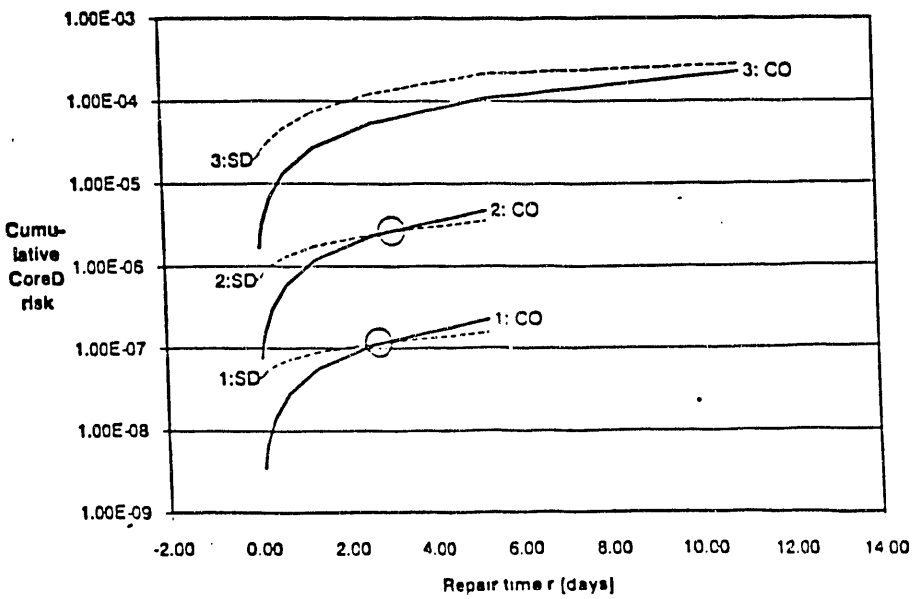

Figure 2b. Cumulative risk over predicted repair time in failures of SSW trains. For example, 2:CO denotes the continued operation alternative when two SSW trains are inoperable [1].

2.3. Contributors to the Shutdown Risk

The risk peak in the SD curve of the instantaneous risk frequency, (Figure 2.a), or equivalently, the nonzero starting value of cumulating risk for SD alternative, (Figure 2.b), represents the risk associated with the change in state of the plant in a controlled shutdown. First of all, it includes the risk of disturbance transients. In the example of SSW failures, the main contributors are:

- loss of normal power-conversion system (PCS) during power reduction or reactor cooldown
- loss of off-site power (LOSP) caused by a shutdown transient

Besides, the risk peak may include the risk of remaining RHR systems failing to start. In the example of SSW failure, this contribution is lacking because the PCS is operating through a smoothly proceeding controlled shutdown, and its use can be extended if the standby RHR systems fail to start.

In the SD alternative, the risk frequency decreases after power reduction, due to diminishing level of decay heat, which allows more time to recovery if a critical failure combination occurs later during the shutdown cooling. Nevertheless, the risk frequency may stay at a substantial level after plant shutdown. In the example of SSW failures, the main contributors during shutdown cooling are:

- loss of instrument air-supply, which, according to operating experiences, has a rather high failure rate in the zero power state
- LOSP, which is especially critical because SSW trains serve also jacket cooling of the diesel generators: therefore, diesel generators are functionally unavailable in those situations where SSW trains are initially detected failed

By comparison, in the example of SSW failures, the risk frequency of the full-power operation state is strongly dominated by LOSP. Thus, the risk profile is rather different from that of a controlled shutdown (SD alternative). It should be emphasized that the risk frequency of the full-power operation state (CO alternative) includes initiating event frequencies and the expected risk of the various kinds of transients and forced shutdowns associated with the initiating events. These details of risk modelling are further discussed in References [1,3].

2.4. The Influence of AOT on the Expected Addition to Risk

The influence of an AOT on the long-term risk of the plant is measured in terms of the risks associated with failure situations which are composed of the contributions of repairs shorter than AOT with continued operation, and repairs exceeding AOT with plant shutdown. These contributions, named here as delta risk, *dfav*, are illustrated in Figure 3.

If AOT is longer than the mean repair time, a large number of the faults will be repaired in a shorter time than the AOT. This means that the expected contribution of repair time while in power state *dfav_co* saturates to a level corresponding to the risk over mean repair time. On the other hand, if AOT is short, the expected number of LCO shutdowns increases and also the associated risk contribution *dfav_sd*. This value should be added to the previous contribution to achieve a correlation of AOT with the situation-specific risk.

Finally, there are indirect influences, which are harder to evaluate. For example, it could be expected that an AOT shorter than normally needed to complete the repair may have negative side

effects, if attempts are made to repair faults hastily to avoid plant shutdown. These types of influences are not analyzed here.

The actual sum curve, i.e., the delta risk - AOT correlation, may have different forms depending on plant-specific features. It is also rather sensitive to calculation uncertainties, as discussed in detail in Section 3.

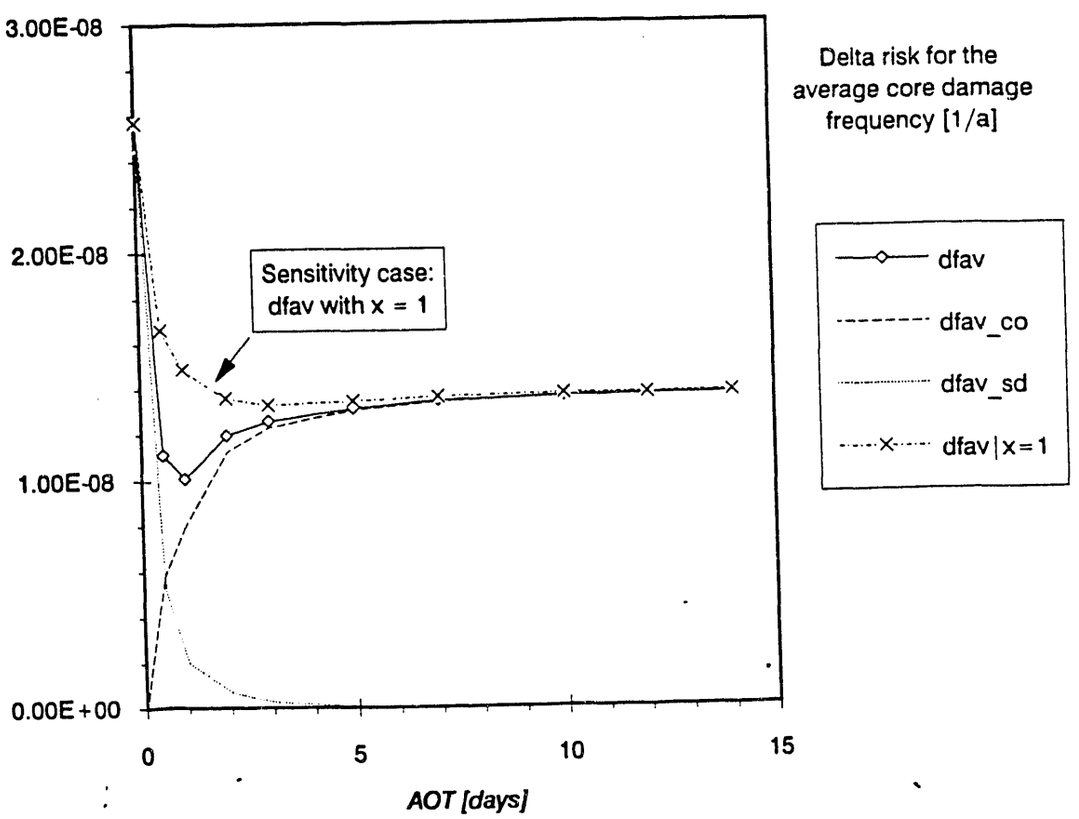

Figure 3. Delta risk - AOT correlation for a double failure of SSW trains [1]. The sensitivity curve was obtained with x=1; namely, giving no credit for repair speed-up. Other correlation curves were obtained with the nominal repair-reduction fraction x=0.5.

3. KEY ISSUES OF THE METHODOLOGY

The main features of our methodology are summarized below. As a complement to earlier presentations, we concentrate here on particular details of the correlation between delta risk and AOT. A more complete presentation of the methodology is included in References [1,3].

3.1. State Modelling Approach

The most essential methodological development relates to the use of Extended Event Sequence Diagram (EESD) to describe event sequences, as a substitute for the traditional event tree/fault tree approach. EESD incorporates intermediate and stable process states which enhances time-dependent modelling of operational scenarios and recovery paths. The latter is viable for a realistic quantification of the decreasing risk (frequency) level while in zero power, due to the diminishing production of decay heat (the prime motivation for a LCO shutdown). Figure 1 is a simple example of EESD, showing some aspects of the approach, especially the use of an embedded state (refer to the state block, "Increased risk, full power state, 2 SSW trains under repair"). In this EESD-based approach, existing PRA models are extremely useful both for the construction of event scenarios, and in modelling of system details.

Connected with the modelling of process states and recovery paths is the necessity of parallel modelling of process behavior, such as the changes in temperature of the suppression pool in a BWR plant, because this is an essential heat buffer, allowing substantial time to recovery in cases where RHR function is lost. Also, development was required to more consistently handle repair and recovery time-distributions, especially in multiple failure situations where alternative recovery paths are available.

3.2. Data Requirements

The data input needed is, to a large extent, similar to that for a PRA study. Additionally, special data are required for modeling the likelihood of disturbance transients during a controlled shutdown, and for the distributions of repair and recovery time.

3.3. Influence of a Preset AOT

A preset AOT, evidently, influences the distribution of repair time, especially when AOT is near to the mean repair time, because the operators then are certainly looking for ways to speed up repairs to avoid plant shutdown. The possibilities include shortening the time spent on administrative tasks, as well as giving a high priority to critical repairs while postponing other, less urgent work.

3.3.1. Influence on Distribution of Repair Time

The influences observed in the early Finnish-Swedish DG study [6] are reproduced in Figure 4. Based on these insights, the following influence model was developed [1]:

- quite soon after the detection of failure, the operators are able to determine the severity class of the repair
- the severity class is described by an exponential repair-time distribution, which, to a certain extent, covers the variability and uncertainty of predicting repair time
- under AOT constraint, the operators/maintenance staff can shorten the repair time to a specific fraction x, from the beginning if the AOT is less than the mean time for the repair severity class,

otherwise, from the time point when the remaining AOT equals the mean repair time. Nominally, fraction x = 0.5 has been used in sensitivity analyses.

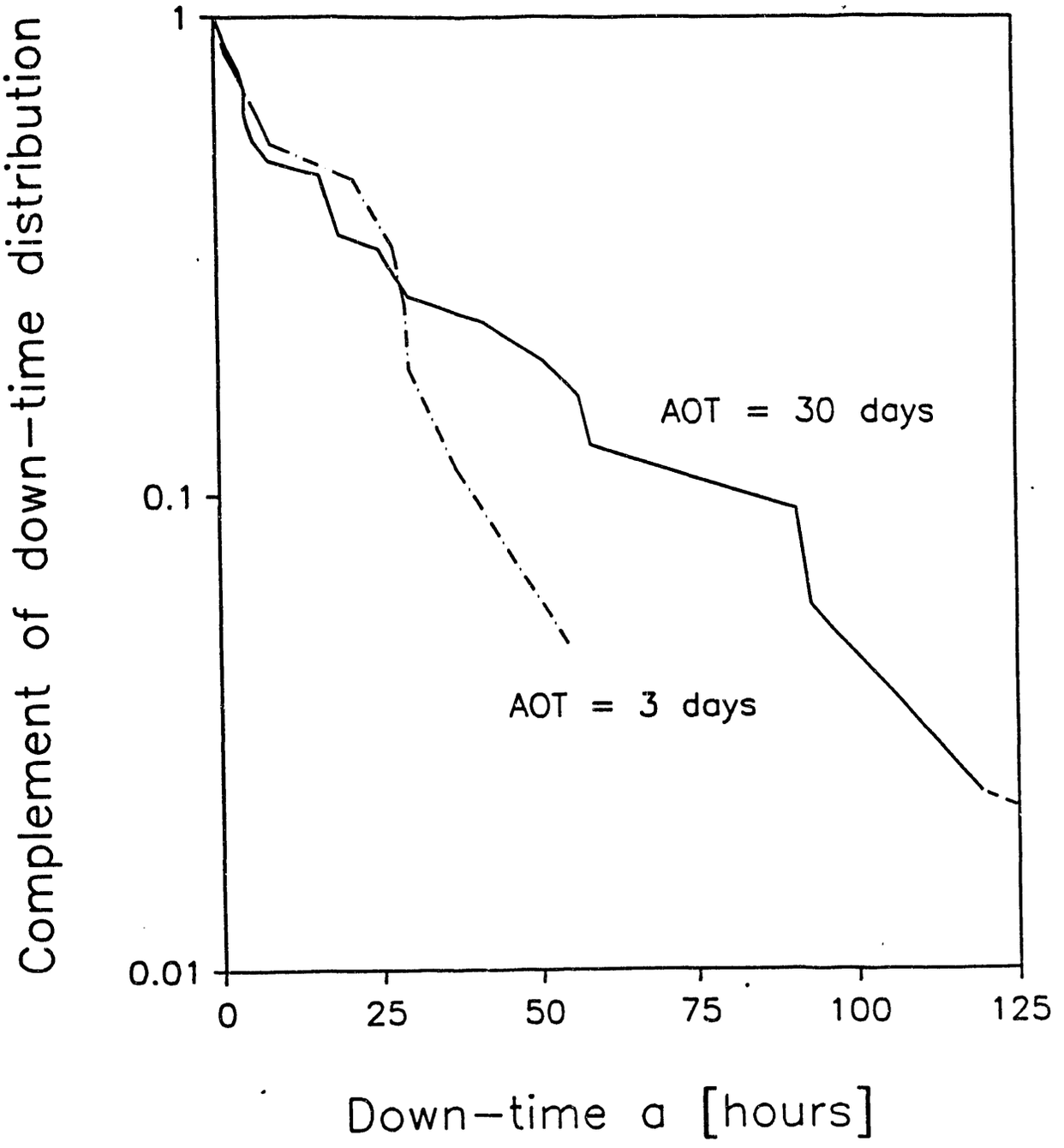

Figure 4. Effect of AOT on the down-time distributions for critical faults of diesel generators [6].

3.3.2. Delta Risk - AOT Correlation

The delta risk contribution, *dfav*, for a specific failure situation, *X*, can be derived from the following breakdown (compare with Figures 1 and 3):

$$dfav_X(AOT) = dfav\_co_X(AOT) + dfav\_sd_X(AOT) \quad (1)$$

where,

$$dfav\_co_X(AOT) = \lambda_X \cdot [\, 1 - pnr_X(AOT) \,] \cdot rco_X(AOT)$$

$$dfav\_sd_X(AOT) = \lambda_X \cdot pnr_X(AOT) \cdot rsd_X(AOT)$$

$rco_X(AOT)$ = P{CoreD| Initiating event occurs during full power repair state}

$$= \frac{\int_0^{AOT} da.fco_X(a).pnr_X(a)}{1 - pnr_X(AOT)} \quad (2)$$

$rsd_X(AOT)$ = P{CoreD| Initiating event occurs during a controlled LCO shutdown or while in the cold shutdown repair state}

$$= \frac{\int_{AOT}^{\infty} da.fsd_X(a).pnr_X(a)}{pnr_X(AOT)} \quad (3)$$

where

λ_X = Rate of the failure situation X

$fco_X(a)$ = Instantaneous risk frequency during full power repair state

$fsd_X(a)$ = Instantaneous risk frequency during a controlled LCO shutdown and while in the cold shutdown repair state

$pnr_X(a)$ = Complementary repair time distribution, i.e. probability of nonsuccessful repair up to time a

The risk here is associated to the core-damage event, CoreD, as is usual in Level-1 PRA. An example of the calculated delta risk - AOT correlation is presented in Figure 3. Besides the nominal repair-reduction fraction x = 0.5, we also show the case of x = 1, i.e. no credit for repair speed-up.

In many cases, the minimum in the delta risk - AOT correlation curve is not very pronounced. The essential conclusion, then, is that if AOT is reasonable in comparişon with a normal possibility of repair, i.e., longer than about three times the mean repair time, the delta risk becomes insensitive to AOT. This conclusion is based on the assumption that there is no significant relaxation in the repair process for long AOTs. It must be emphasized that the plant staff should have a strong motivation to carry out repairs without unnecessary delays, even with long AOTs, because this reduces the possibility of occurrence of complex multiple failures.

3.4. Sensitivity Analysis to Address Uncertainties

The uncertainties in the AOT considerations, and especially in the risk-comparison approach described here, are similar to PRA studies and other risk-based applications. Additional uncertainties

may be related to the specific modelling features and data requirements discussed in Sections 3.1 and 3.2; i.e., in obtaining probability estimates for disturbance transients, and repair or recovery time distributions.

Importantly, in using the risk-comparison approach, the relative results matter, and, to a large part, they often are not very sensitive to uncertainties. For important uncertainties, systematic sensitivity analysis can be used to verify conclusions; an example is shown in Figure 5.

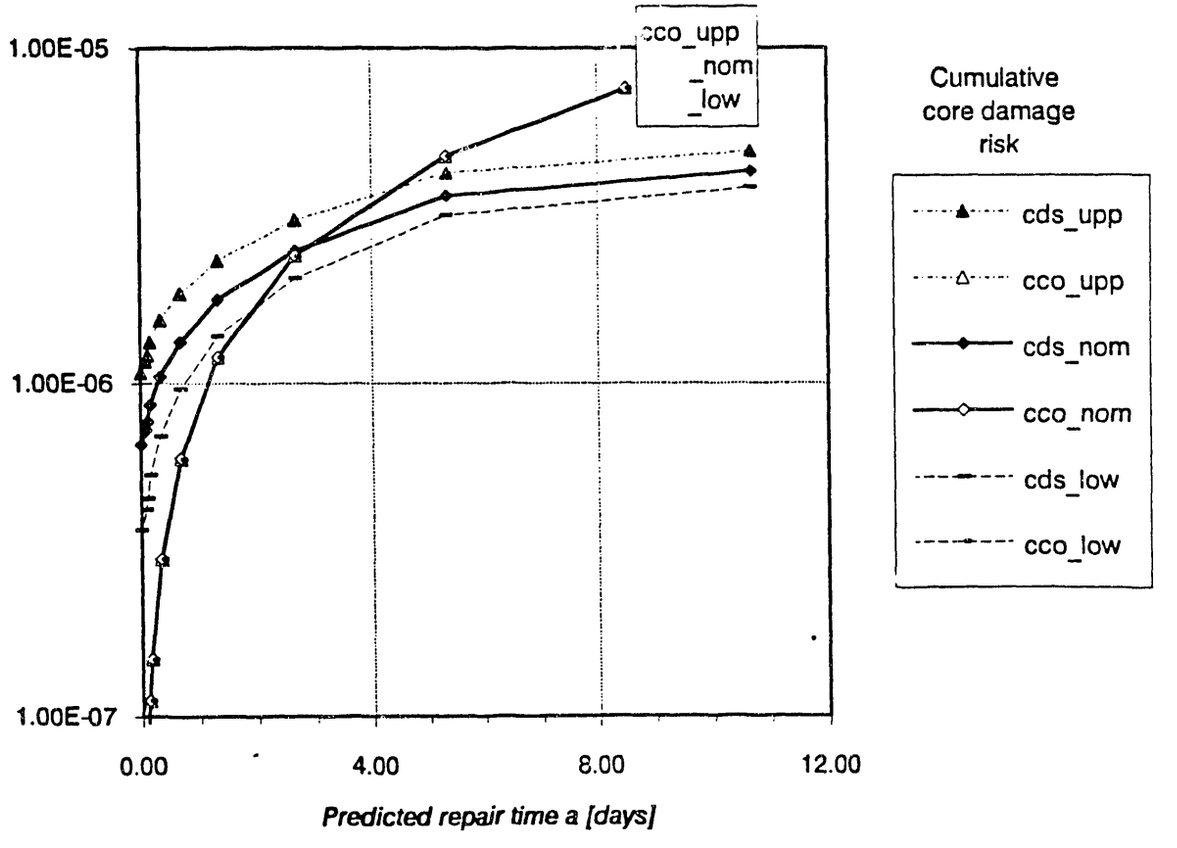

Figure 5. Sensitivity of cumulative core-damage risk in a double failure of SSW trains for the likelihood of disturbance transients in a controlled shutdown (variation factor = 3).

4. CONCLUSIONS

This risk-comparison approach and methodology is needed to properly infer how the predicted risk of the plant shutdown alternative compares with making repairs in a full-power operation state. The approach is especially important when determining AOTs for the systems related to decay-heat removal function, because plant shutdown with degraded capability to remove decay heat can result in a substantial risk, based on the results from our case studies.

The insights obtained lead to suggestions for modifying operational details of TS action statements. The timing and desired end-state of the LCO shutdown (i.e., the state of the system in which to undertake the bulk work of repairs) may need to be optimized.

Experiences show that the results of risk-based AOT considerations depend on many plant-specific features, such as vulnerability to disturbance transients during a controlled shutdown, and the operational reliability of the systems to be used while in zero-power state. Therefore, it must be emphasized that the results from the pilot study, used here to illustrate the approach and methodology, should not be regarded as generally applicable.

REFERENCES

1. Risk-based improvement of Technical Specification action statements requiring shutdown: Pilot application to the RHR/SSW systems of a BWR. Prepared for U.S. Nuclear Regulatory Commission by T. Mankamo, I.S. Kim and P.K. Samanta, in preparation.

2. Mankamo, T. and Kosonen, M., Operational decision alternatives in failure situations of standby safety systems. IAEA Technical Committee Meeting on The Use of PSA to Evaluate NPP's Technical specifications, Vienna, 18-22 June 1990.

3. Mankamo, T. and Kosonen, M., Continued plant operation versus shutdown in failure situations of standby safety systems, application of risk analysis methods for the evaluation and balancing of AOTs for the RHR systems at TVO I/II plant. IAEA/Tech Spec Pilot Study Program NKS/SIK-1(91)4, August 1991.

4. Vesely, W. and Samanta, P.K., Risk Criteria Considerations in Evaluating Risks from Technical Specification Modifications. Technical Report, BNL & SAIC, Draft, January 1989.

5. Optimization of technical specifications by use of probabilistic methods - a Nordic perspective. Final report of the NKA project RAS-450. Ed. K. Laakso. Prepared by K. Laakso, M. Knochenhauer, T. Mankamo and K. Pörn. Nord. Series 1990:33, May 1990.

6. Pulkkinen, U., Huovinen, T., Mankamo, T., Norros, L. and Vanhala, J., Reliability of diesel generators in the Finnish and Swedish nuclear power plants. Technical Research Centre of Finland, Report SÄH 7/82, June 1982. (Enhanced version published as VTT Research Notes 1070, 1989)

7. Hioki, K. and Kani, Y.,Risk based evaluation of technical specifications for a decay heat removal system of an LMFBR plant. IAEA Technical Committee Meeting on The Use of PSA to Evaluate NPP's Technical specifications, Vienna, 18-22 June 1990.

END

DATE
FILMED
5/7/93