

Hazard Rate for a Two-Channel Protective System Subject to a High Demand Rate*

L. F. Oliveira, R. Youngblood
Brookhaven National Laboratory, Upton, NY USA

P. F. F. Melo
COPPE/UFRJ, Rio de Janeiro, RJ, Brazil

INTRODUCTION

A basic figure of merit associated with a protective system for an industrial plant is the number of accidents expected to occur in the plant within a given period of time, with the system installed. By definition, in a plant equipped with a protective system, an accident can only happen if an initiating event (a demand) occurs while the protective system is unavailable, that is, while it is in one of its possible failed states. This means that the hazard rate or accident frequency depends on the demand rate and on the unavailability of the protective systems. It has long been recognized that the demand rate influences the unavailability of the protective system, and practical expressions incorporating that effect have been developed for single-channel (Lees, 1982) and multi-channel (Kumamoto and Henley, 1978) protective systems. The effect has also been incorporated into a Markovian treatment of a plant protection system (Papazoglou and Cho, 1985). In a previous paper (Oliveira and Netto, 1987) a Markovian approach was used to derive analytical expressions for the evaluation of the plant hazard rate for a single-channel protective system, properly accounting for the effects of the demand and the repair rates. In this paper, we present an extension of that model to the case of a plant equipped with a two-channel protective system.

TWO WAYS TO MODEL THE PROBLEM

General Assumptions

The protective systems analyzed in this work are considered to be formed by two redundant independent channels with identical failure and repair characteristics, and exponentially distributed times to failure and repair. The mission success criterion assumed here is that if one of the two channels is operational when a demand occurs, then the system will work as required (one out of two: good). Both channels are subject to periodic testing at proof test intervals of duration t_p . Failed states of either channel are always detected by tests (Perfect tests) and the channels are renewed to as-good-as-new conditions after testing. The test duration is negligible compared to the proof test interval. The demand rate is considered to be constant in time.

Model 1: Failure of a Single Channel Not Revealed by Demand

In Model 1, the status of a failed channel is not revealed to the operators if the protective function is successfully performed by the other channel; only

*This work is based on work performed under the auspices of the U.S. Department of Energy.

the periodic proof tests are capable of revealing the status of each separate channel. Therefore, in case of a demand, repair activities will not be conducted unless both channels are failed, that is, unless the system is down. This assumption leads to the state diagram shown in Fig. 1. Two cases can be considered: (1) after an accident, the plant is offline until the protective system is repaired, so that challenges are precluded or (2) the plant is allowed to resume operation after an accident, even while the protective system is under repair. It can be shown that plant hazard rates for these two cases are given by:

$$\eta = \delta \bar{P}_3 \quad \text{and} \quad \eta = \delta(\bar{P}_3 + \bar{P}_4) \quad (1)$$

respectively, where

$$\bar{P}_i = \frac{1}{\tau_p} \int_0^{\tau_p} P_i(t) dt \quad (2)$$

Model 2: Failure of a Single Channel Revealed by Demand

In this model it is assumed that the failed state of a single channel is revealed to the operators in case of occurrence of a demand, despite the fact that the protective system as a whole will operate successfully, resulting in no plant hazard. This means that the operators can proceed to repair the failed channel with the plant on line while still maintaining the safety margin afforded by the remaining operational channel.

The state diagram corresponding to this model is shown in Fig. 2, where the availability of two repair crews is assumed. Following the same reasoning used for Model 1, the plant hazard rate for Model 2 can be defined by:

$$\eta = \delta(\bar{P}_3 + \bar{P}_4 + \bar{P}_5) \quad (3)$$

or by

$$\eta = \delta(\bar{P}_3 + \bar{P}_5) \quad (4)$$

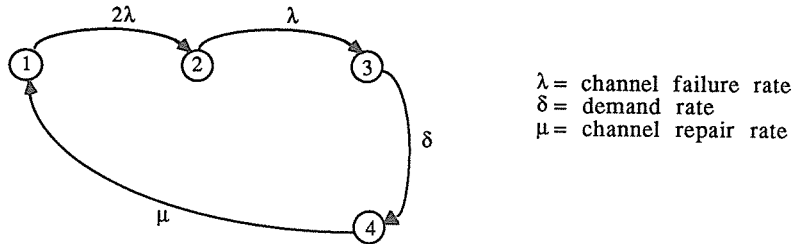
DISCUSSION OF RESULTS

In this work, the corresponding system of differential equations has been numerically solved using the exponential matrix method, for a time period equal to the proof test interval, τ_p , with initial conditions $P_1(0) = 1$, and $P_2(0) = P_3(0) = P_4(0) = 0$. Results for both models are shown in Fig. 3.

The results for Model 1 accord with simple intuition. Repair makes it possible to have more accidents because the system is up and running again after the first accident, but with increasing demand rate, the accident rate eventually saturates at a limiting value because there is only time for so many accidents within a given year (for a given combination of repair times and failure rates).

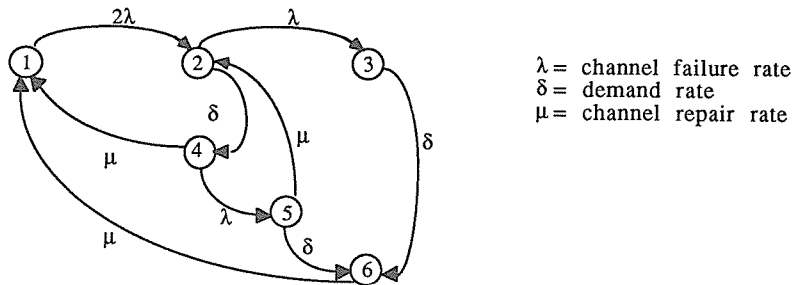
An interesting aspect of Model 2 is the variation of the predicted hazard rate with respect to the demand rate. Refer to Fig. 3. Two features of Model 2's hazard rate are noteworthy: first, it tends to an asymptotic value, and second, it has a maximum. The maximum in the hazard rate results from the conflicting roles which are played by demands in this model: on one hand, a demand may initiate an accident, and on the other, it provides a kind of monitoring capability of the status of each component with immediate initiation of repair in case of failure detection (a "recovery capability"). Therefore, an increase in demand rate has competing effects on the hazard rate, with the final variation in hazard rate being dictated by the balance of these

Figure 1 - State diagram for Model 1



- State 1: Both channels are up
- State 2: One channel is up, and the other is down but failure is undetected
- State 3: Both channels are down, but failures are undetected
- State 4: Both channels are under repair, their failures have been detected due to the occurrence of a demand

Figure 2 - State diagram for Model 2

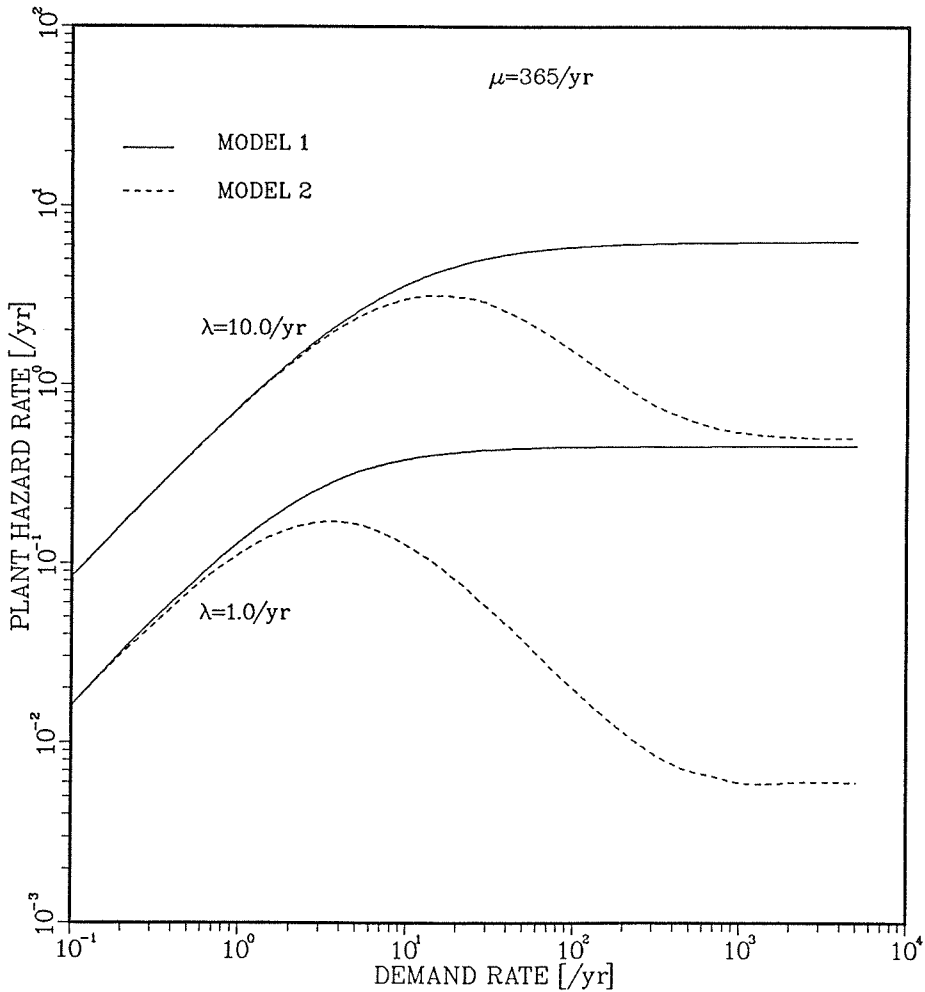


- State 1: Both channels are up
- State 2: One channel is up, and the other is down but failure is undetected
- State 3: Both channels are down, but failures are undetected
- State 4: One channel is up, the other is down (failure detected due to a demand)
- State 5: One channel is down but undetected, and the other is under repair
- State 6: Both channels are under repair, their failures have been detected due to a demand

two effects. For low values of δ , the recovery capability is not effective and consequently η increases with δ , but after some point (which depends on λ and μ), the recovery capability begins to dominate the balance, and further increases of δ result in an actual decrease of η .

In the limit of very large δ , the logic of both Models 1 and 2 simplifies to the extent that analytic expressions for the asymptotic plant hazard rate can be derived, as shown in Oliveira et al., 1989; the discussion proceeds by mapping the large- δ limit of Model 2 onto a previously solved problem involving continuous monitoring of system channels.

FIGURE 3 - PLANT HAZARD RATE VS DEMAND RATE



COMPARISON WITH OTHER MODELS

It is useful to compare the results of our models with those obtained by Kumamoto and Henley, 1978, and those of Lees, 1982, which also explicitly considered the effect of the demand rate on system unavailability. Elsewhere (Oliveira et al., 1989), it is shown that their expressions can be obtained as limiting results of our models for the case of no repair of the failed channels. It turns out that for much of the range of practical interest of the relevant parameters (λ , δ , and τ_p) the results of the existing analytical expressions for $\mu = 0$ are sufficiently accurate to be used even when μ is much greater than zero. However, significant differences appear in the high end of the range of parameters, especially for high values of $\delta\tau_p$.

For simplicity, the analyses presented here use the same repair rate for repairing accident damage that is used for repair of failed individual channels. If it is assumed that an accident would demolish the facility beyond any possibility of repair, the corresponding transition rate for the accident repair arc is zero; in this case, there is no return from the state corresponding to an accident having occurred, and this state is therefore an "absorbing state." In some parameter regimes, treating the accident state as "absorbing" has a significant effect on the computed hazard rate; clearly, the true hazard rate of such a facility cannot exceed unity (in any system of units), because the facility will have at most one accident in any time interval. Thus, modelling the recovery from an accident is critical in parameter regimes corresponding to hazard rates which are significant compared to unity. For hazard rates which are much less than unity, the computed hazard rate is not significantly affected by the accident repair arc.

In the absorbing state version of the model, the time-averaged hazard rate can be identified with the probability of being in the absorbing state at the conclusion of the time interval over which the computation is performed. This follows because the occupation of the absorbing state is given by the integral over time of the instantaneous hazard rate. From Eq. (2), it is seen that these quantities are simply related to the time-averaged occupancies of those states from which it is possible to transit directly to the absorbing state. However, this identification of a hazard rate with absorbing state occupancy is possible only in the absorbing-state limit; if there is any possibility of plant operation after an accident, there is no longer a simple relationship between the hazard rate and the occupancy of the state "under repair following accident."

CONCLUSIONS

The effect of on-line repair on system figures of merit can be quite dramatic. Even in the simple models considered here, the effect of repair is not simple: a decrease in hazard rate with an increase in demand rate would be difficult to predict within the framework of a fault tree treatment. It is particularly interesting that these complexities are observed for parameter values which are typical of realistic applications. In not taking account of the effect of system demands on system restoration, an oversimplified analysis can easily overstate the hazard rate. Correspondingly, by monitoring only the performance of a safety function, and not the performance of individual channels (in short, by actualizing Model 1 rather than Model 2), plant operators can miss an opportunity to reduce significantly the plant hazard rate.

REFERENCES

- Lees, F. P. (1982). "A General Relation for the Reliability of a Single-Channel Trip System, Reliability Engineering, 3(1), p. 1.
- Kumamoto, H. and Henley, E. J. (1978). "Protective System Hazard Analysis," Ind. Eng. Chem. Fundam., 17(4).
- Papazoglou, I. A. and Cho, N. Z. (1985). "A Markovian Analysis of Limiting Conditions of Operation for the Reactor Protection System," Proc. ANS/ENS International Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, CA, February 24-March 1, 1985 (Electric Power Research Institute).
- Oliveira, L. F. and Netto, J. D. (1987). "Influence of the Demand Rate and Repair Rate on the Reliability of a single-Channel Protective System," Reliability Engineering, 17(4), p. 267.
- Oliveira, L. F., Youngblood, R., and Melo, P. F. F. (1989). "Hazard Rate of a Plant Equipped with a Two-Channel Protective System Subject to a High Demand Rate," to be published in Reliability Engineering and System Safety.