Journal of the Korean Nuclear Society
Volume 23, Number 2, June 1991

Effects of Human Error on the Optimal Test Interval and Unavailability of the Safety System

Dae Wook Chung and Bon Hyun Koo
Korea Institute of Nuclear Safety
(Received October 10, 1990)

안전계통의 이용불능도 및 최적시험주기에 미치는 인간실수의 영향

정대욱 · 구본현
한국원자력안전기술원
(1990. 10. 10 접수)

Abstract

Effects of human error relevant to the periodic test are incorporated in the evaluations of the unavailability and optimal test interval of a safety system. Two types of possible human error with respect to the test and maintenance are considered. One is the possibility that a good safety system is inadvertently left in a bad state after test(Type A human error) and the other is the possibility that a bad safety system is undetected upon the test (Type B human error). An event tree model is developed for the steady-state unavailability of a safety system in order to determine the effects of human errors on the system unavailability and the optimal test interval. A reliability analysis of the Safety Injection System (SIS) was performed to evaluate the effects of human error on the SIS unavailability. Results of various sensitivity analyses show that ; (1) the steady-state unavailability of the safety system increases as the probabilities of both types of human error increase and it is far more sensitive to Type A human error, (2) the optimal test interval increases slightly as the probability of Type A human error increases but it decreases as the probability of Type B human error increases, and (3) provided that the test interval of the safety injction pump is kept unchanged, the unavailability of SIS increases significantly as the probability of Type A human error increases but slightly as the probability of Type B human error increases. Therefore, to obtain the realistic result of reliability analysis, one should take shorter test interval (not optimal test interval) so that the unavailability of SIS can be maintained at the same level irrespective of human error. Since Type A human error during test & maintenance influeces greatly on the system unavailability, special efforts to reduce the possibility of Type A human error are essential in the course of test & maintenance.

요 약

안전계통의 이용불능도 및 최적시험주기 평가에 있어서 주기적인 시험과 관련된 인간실수의 영향을 고려하였다. 시험 및 보수와 관련된 인간실수는 건전한 계통이 시험후 잘못된 상태에 놓이게 될 가능성과(Type A 인간실수) 건전하지 못한 계통이 시험시 감지되지 못할 가능성(Type B 인간실수)이다. 계통이용불능도 및 최적시험주기에 미치는 인간실수의 영향을 결정하기 위하여 안전

계통의 이용불능도를 계산하기 위한 사상수목모델이 개발되었다. 또한 안전주입계통의 신뢰도 분석을 통하여 계통전체에 미치는 영향을 평가하였다. 다양한 민감도 분석 결과, (1) 계통이용불능도는 인간실수의 확률이 커질수록 증가하며 Type A 인간실수의 영향이 훨씬 크다. (2) 최적시험주기는 Type A 인간실수가 커질수록 약간 증가하나, Type B 인간실수가 커질수록 감소한다. (3) 안전주입펌프의 시험주기를 고정시키면 안전주입계통의 이용불능도는 Type A 인간실수가 커질수록 크게 증가하나 Type B 인간실수가 커지더라도 약간 증가한다. 따라서 인간실수의 영향을 고려할 때 계통의 이용불능도를 일정 수준으로 유지하기 위해서는 시험주기(최적시험주기가 아님)를 줄여야 한다. 그리고 시험 및 보수시 Type A 인간실수는 계통의 이용불능도에 미치는 영향이 크므로, 특히 Type A 인간실수를 줄이기 위한 노력이 필요하다.

1. Introduction

There have been growing efforts to modify the technical specifications of nuclear power plant, especially the surveillance test intervals (STI's) by using Probabilistic Safety Assessment (PSA) technique. Technical Sepcifications are intimately related to risk because they establish the minimum functional requirements for the safety systems that are responsible for protecting the plant in the event of an abnormal operating condition. Surveillance requirements specify test and inspection procedures that assure the quality of safety limits, limiting safety system settings, and LCO's. The surveillance test intervals are the minimum required time intervals that major safety systems should be under the inspection or test to insure their availability for use when needed. Test frequencies that are based on engineering judgement may not be optimized from a safety standpoint. Test frequencies that are too short result in excessive radiation exposure to plant personnel and possibly increase risks of test-induced plant transient. Test frequencies that are too long do not provide adequate assurance for protecting public safety. They can be relaxed only when the relaxation has no significant effect on the system availability and/or core melt frequency. At present, it is reported that test interval for major component of some safety systems can be relaxed via the system reliability analysis.[2],[3]

However, the possibility of human error during test and maintenance of such component of safety systems is obviously present and the effects of human error should be incorporated in the system reliability study in order to avoid the underestimation of system unavailability. Human error effects have not been explicitly accounted for in determining the STI's.

Two types of human error are possible with respect to the testing. One is the possibility that a good safety system is inadvertently left in bad state after inspection (Type A human error). Such has been cited in regard to TMI-2 accident, i.e., a manual isolation valve may be inadvertently left in a closed position after the test on an auxiliary feedwater system. The other type of possible human error is that a bad safety system is undetected on inspection (Type B human error). The inclusion of human error in the development of appropriate inspection plans or procedures has recently been undertaken. Thereby, optimal test interval and the system availability can be derived more realistically The safety system unavailability as well as the optimal test interval is proven to be susceptible to human error.

Here, such human errors are considered in calculating the steady-state unavailability and optimal test interval of safety system by using a simple event tree model for the calculation of steady-state unavailability of the safety system. Such a consideration is already undertaken by T.P.McWil-

liams and H.F.Martz by using a Markov model.[1] Conclusively, the reliability analysis of safety injection system (SIS) is performed to evaluate the effects of human error on SIS unavailability. Details of the analysis are provided in the following sections.

2. Steady-state Unavailability

The steady-state unavailability of a safety system without human error can be written as;

$$Q=Q_i+Q_{CCF} \qquad E_q.(1)$$
$$=(Q_S+Q_{TM}+Q_{etc})+Q_{CCF}$$

where

Q_i : average unavailability due to independent failure,

Q_{CCF} : average unavailability due to common cause failure,

Q_S : average unavailability due to failure during standby,

Q_{TH} : average unavailability due to test and maintenance, and

Q_{etc} : average unavailability due to others.

Now, we can calculate each term with the fundamentals in reliability study. The probability that a system fails after time t is given by:

$q(t)=1-e^{-\lambda t}$

where λ is failure rate of the system(time^{-1}) Hence, the average unavailability during the test interval T is calculated by;

$$Q_S=\frac{1}{T}\int_0^T q(t)dt$$
$$=\frac{1}{T}\int_0^T(1-e^{-\lambda t})dt$$
$$=1-\frac{1}{\lambda T}(1-e^{-\lambda T}) \qquad Eq.(2)$$

If $\lambda T<<1$, then

$$Q_s\cong\frac{1}{2}\lambda T$$

The unavailability due to the test & maintenance is calculated by;

$$Q_{TM}=Q_{Test}+Q_{Maintenance}$$
$$=\frac{t_1}{T+t_1}+F\frac{t_2}{T+t_1+t_2} \qquad Eq.(3)$$

where

t_1 : test time

t_2 : maintenance time

F : average maintenace frequency.

Common cause failure can be included by using the β-factor method. β-factor is defined as the ratio of common cause failure rate to the total failure rate. Common cause failures are very important factor in reliability analysis, and there are various methodologies to treat the common cause failures. Above all, β-factor method is the most popular one because of its simplicity and direct applicability to large fault tree analysis. Irrespective of its deficiency in treating the multiple dependent failures separately, i.e., double or triple dependent failures are not separable and all components in redundant system fail simultaneously due to a common cause initiating event or a shock, this method is adopted in this study because the CCF does not affect the result of this study. By definition, the β-factor is

$$\beta=\frac{Q_{CCF}}{Q}=\frac{Q_{CCF}}{Q_i+Q_{CCF}}$$

Hence,

$$Q_{CCF}=\frac{\beta}{1-\beta}Q_i \qquad Eq.(4)$$

Beta factor of 0.17 will be used for safety injection pump in the reliability analysis of safety injection system (SIS) afterwards.[6]

Finally we can obtain the steady-state unavailability by substituting above results into Eq.(1). Assuming that the unavailability due to others is negligible, then Eq.(1). can be rewritten as

$$Q=Q_T+Q_{CCF}$$
$$=(Q_{SH}+Q_{TM})+Q_{CCF} \qquad Eq.(5)$$

where

Q_{SH} : *unavailability due to both random failure* and human error relevant to test & maintenance.

cess is given by;

$$Q_1 = P_A e^{-\lambda T} \qquad \text{Eq.(6)}$$

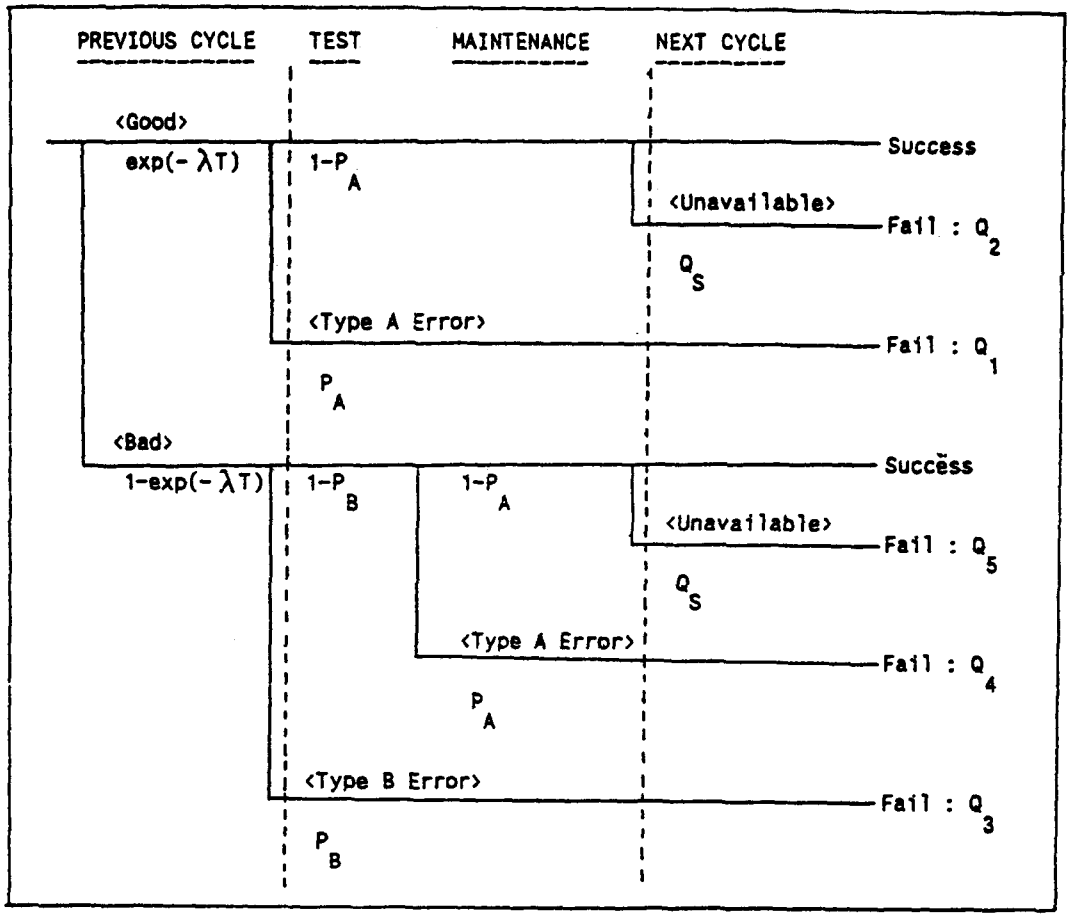

Fig.1. Event Tree for Pump Unavailability Including Human Errors during Test

Now, we should find the average unavailability with human error, Q_{SH}. An event tree is developed as shown in Fig.1 to evaluate the unavailability of a safety system during standby after test. At the beginning of test or after the previous cycle, the system is in either good or bad state. The probability of being each state is $e^{-\lambda T}$ and $1-e^{-\lambda T}$, respectively. If the system is good, Type A human error can be possible and the probability that the system is unavailable following this process is given by;

$$Q_1 = P_A e^{-\lambda T} \qquad \text{Eq.(6)}$$

Suppose that a good system remains still good state after test, system can be unavailable due to the failure during standby for the next test interval after test. The probability that the system is unavailable following this process is obtained by;

$$Q_2 = (1-P_A) Q_S e^{-\lambda T} \qquad \text{Eq.(7)}$$

where Q_S is expressed in Eq.(2).

If the system is bad, Type B human error can be possible and the probability that the system is

unavailable following this process is given by;

$$Q_3=P_B(1-e^{-\lambda T}) \quad \text{Eq.(8)}$$

Suppose that a bad system be detected upon test, the system should be repaired. After repair, the system will be subjected to test and Type A human error can be possible. The probability that the system is unavailable following this process is

$$Q_4=P_A(1-P_B)\,(1-e^{-\lambda T}) \quad \text{Eq.(9)}$$

If both types of human error did not occur, the system can be unavailable due to the failure during standby for the next test interval after the test, that is

$$Q_5=(1-P_A)\,(1-P_B)\,Q_S(1-e^{-\lambda T}) \quad \text{Eq.(10)}$$

Finally, we get from Eq.(6) through Eq.(10);

$$\begin{aligned} Q_{SH} &= Q_1+Q_2+Q_3+Q_4+Q_5 \\ &= P_Ae^{-\lambda T}+(1-P_A)Q_Se^{-\lambda T} \\ &\quad +P_B(1-e^{-\lambda T})+P_A(1-P_B)(1-e^{-\lambda T}) \\ &\quad +(1-P_A)(1-P_B)Q_S(1-e^{-\lambda T}), \end{aligned} \quad \text{Eq.(11)}$$

and

$$Q_T=Q_{SH}+Q_{TM} \quad \text{Eq.(12)}$$

whe Q_S and Q_{TM} are expressed in Eq.(2) and Eq.(3). One can easily find that the average unavailability of the system without human error, Q_S, by setting the probabilities for both types of human erros equal to zero in Eq.(11).

Eq.(12) expresses the average unavailability of the system with human errors of Type A and B.

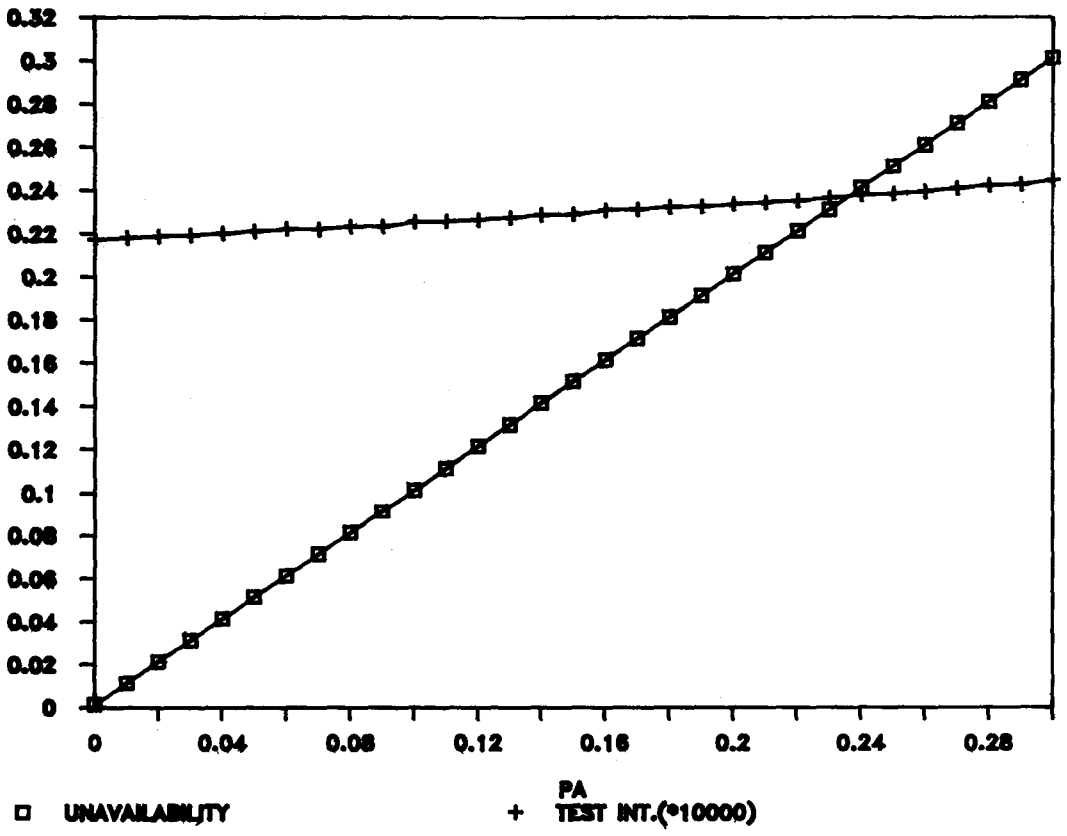

Fig.2. Optimal Condition with Type A Human Error

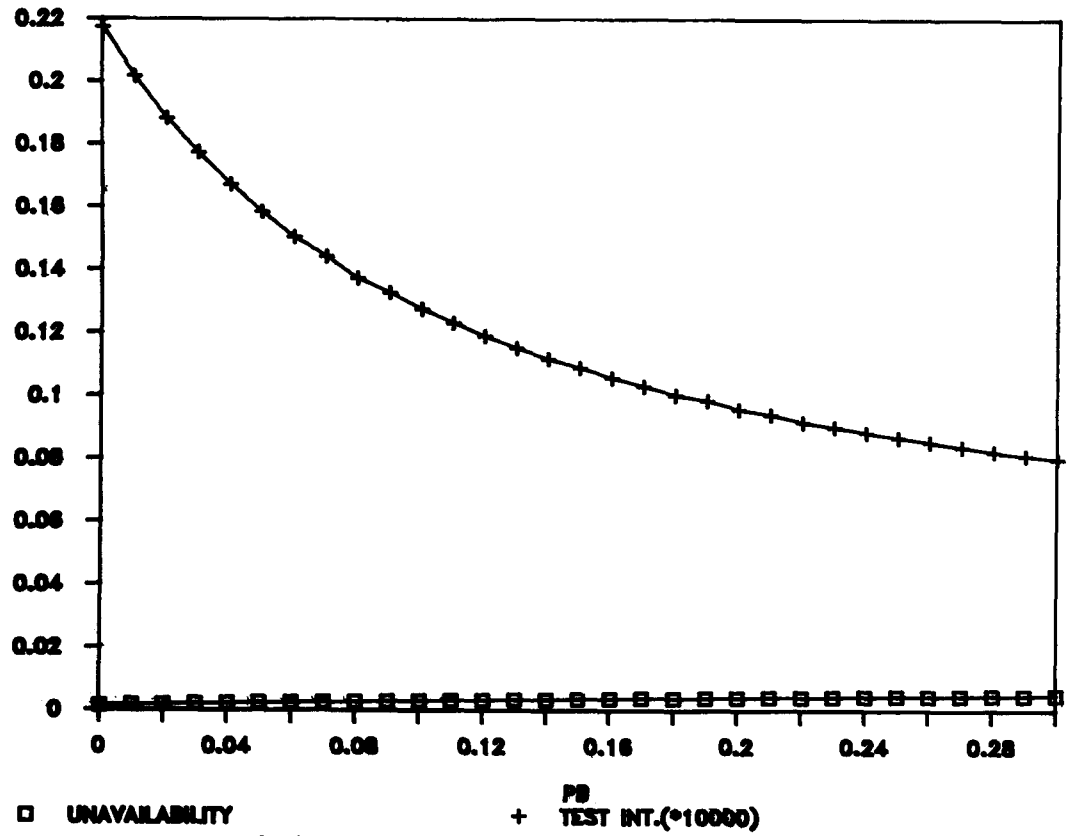

Fig.3. Optimal Condition with Type B Human Error

Q_T varies with the probabilities of both types of human error and with the test interval T, given that λ is constant. The optimal test interval is the test interval which minimize the unavailability or test cost of the system. Here, we derive it with respect to the unavailability. Thus the optimal test interval is derived from this equation by setting the derivative of Eq.(12) with T equal to zero. The optimal test interval and associated average unavailability are plotted in Fig.2 and Fig.3 by varying the probability of Type A and Type B, respectively. The test time of 2 hours and λ of 10^{-5} hr^{-1} are assumed. From the calculational results, we can find that the optimal test interval increases slightly and the unavailability increases significantly with the probability of Type A human error. On the other hand, the optimal test interval decreases but the unavailability increases slightly with the probability of Type B human error.

The reliability analysis for safety injection system (SIS) of Kori 3 & 4 are performed to evaluate the effects of human error on the total system unavailability in the light of this results.

In general, the surveillance test interval for a safety system is not always the optimal test interval due to some practical reasons and the existence of human error renders the unavailability higher. Therefore, the test interval should be shifted to the direction of optimal test interval so that the unavailability can be maintained at the same level irrespective of human error. The desired test interval can be derived by setting the unavailability with P_A and P_B almost equal to that of the non-human error case, by varying the test interval T, that is

$$\left| \frac{Q_T - Q_O}{Q_T} \right| \leq \epsilon$$

where

Q_0 : unavailability of non-human error case

ϵ : convergence criteria

Q_T : unavailability with P_A and P_B and with varying T

A simple FORTRAN 77 program is written to obtain the desired test interval with the convergence criteria ϵ of 0.01. The results are shown in Fig.4. The desired test interval (not optimal test interval) decreases significantly by including human error and is much more sensitive to Type A human error than Type B human error. Hence, one can easily recognize that the efforts to minimize the probability of Type A human error should be essential.

3. Reliability Analysis of Safety Injection System

We performed the reliability analysis of SIS to evaluate the effects of human error on the total system unavailability. Details of analysis are provided in Reference(4). The safety injection pumps are the key components of SIS whose unavailabilities are the major contributors to the SIS unavailability. The test interval for these pumps is fixed as 2160 hours, which makes the unavailability of the SI pump highter than that of the case with optimal test interval. Considering that the optimal test interval varies with human error probability, the fixed test interval results in even highter unavailability.

We performed the sensitivity analysis of human errors by applying aforementioned unavailability

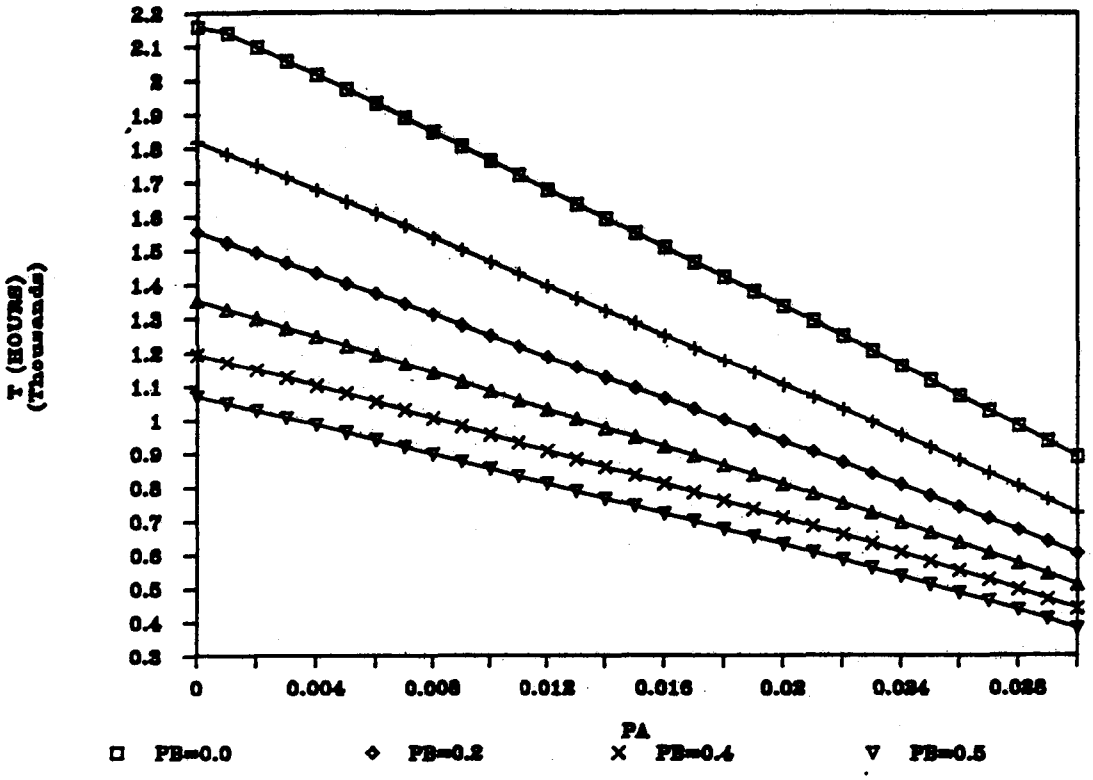

Fig.4. Desired Test Interval vs. Human Errors

model to SI pumps. For convenience, we rewrite Eq.(5) for pump

$$Q_P = Q_{TP} + Q_{CCFP} + Q_{etc.p}$$

where Q_{TP} is obtained from Eq.(12), Q_{CCFP} is obtained from Eq.(4) by equalizing Q_i to Q_{TP}, and last term represents the failures of signal, cooling and control circuit. The simplified safety injection system is shown in Fig.5 and the results of analyses are shown in Fig.6. One can easily find that the unavailability of SIS increases greatly with the unavailability of Type A human error and slightly with the unavailability of Type B human error, which reveals the same trend compared to the unavailability of a safety injection pump. This means that SI pump are the key systems in SIS. Hence, the unavailability of SI pump should be minimized in order to minimize the unavailability of the SIS.

4. Conclusion

In the light of the results from various sensitivity analyses, it is proved that the human errors of both Type A and B influence greatly on the component unavailability and test interval. Consequently, the total unavailability of SIS increases significantly following the inclusion of human errors. Type A human error (that is, a good system is inadvertently left in a bad state after test) has much more important effect on the unavailability. Based on the results of this study, we conclude that

1) The unavailability increases as the human errors are considered and the effect of Type A human error is dominant.
2) The optimal test interval decreases as the probability of Type B human error increases but it increases slightly as the probability of Type A human error increases.
3) To avoid the underestimation of system unavailability, effects of human errors should be incorporated in the system reliability analysis quantitatively which aims at the relaxation of surveillance test interval.
4) The SI pumps are the key safety systems in the SIS and Type A human error has also great

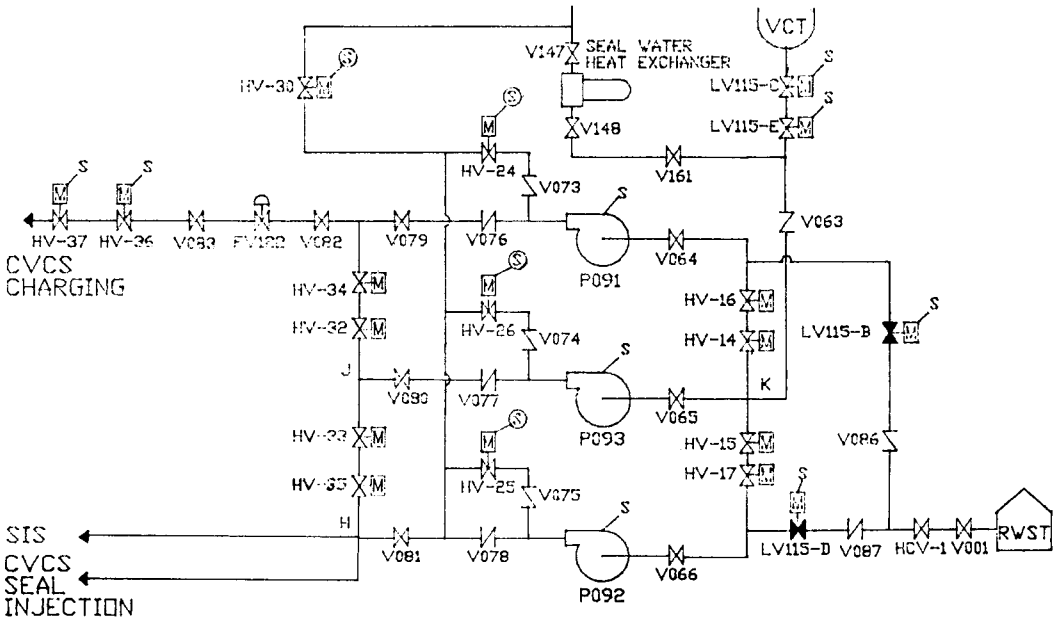

Fig.5. The Safety Injection System

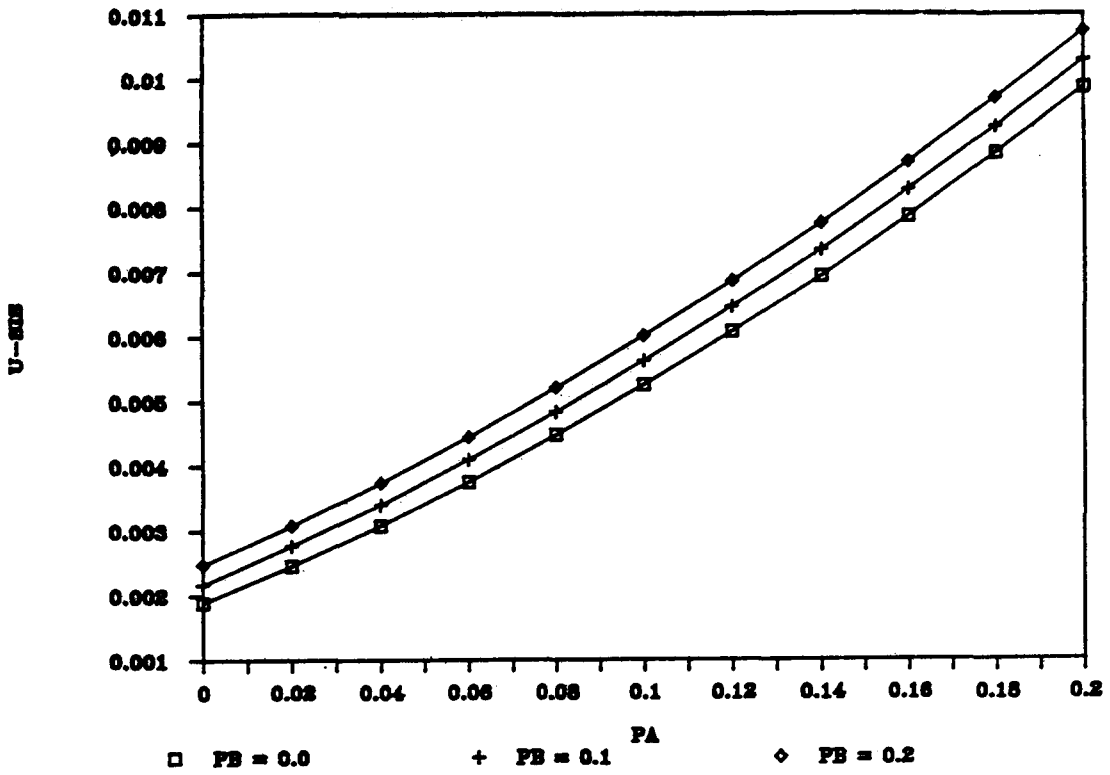

Fig.6. SIS Unavailability vs. Human Errors

effect on the unavailability of SIS. Hence Type A human error during test & maintenance of SI pump should be minimized in order to minimize the unavailability of the SIS.

5) Especially, Type A human error should be considered more adequately not only in the course of reliability analysis but in the test and inspection procedures.
6) To reduce the possibility of human error during the test procedure, possible erroneous situation should be removed in addition to the qualification and training of the personnel.[5]

References

1. T.P McWilliams, H.F. Martz, "Human Error Considerations in Determining the Optimal Test Interval for Periodically Inspected Standby System", IEEE Trans. on Reliability Vol. R-29, No.4, pp.305-310, 1980
2. E.V. Lofgren, F. Varcolik, "Probabilistic Approaches t LCO's and Surveillance Requirements for Standby Safety System", NUREG.CR-3082, 1982
3. D.P. Wagner et al., "Risk-based Evaluation of Technical Specifications", EPRI NP-4317, 1986
4. D.W. Chung et al., "A Reliability Analysis of HHSIS of KNU 5,6,7, and 8 Following the Removal of s-signal from Charging/Safety Injection Pump Mini-flow Line Valves", Journal of Korean Nuclear Society, Vol.20, No.1 pp.47-52, March, 1988.
5. H. Kragt, "Human Reliability Engineering", IEEE Trans. on Reliability, Vol. R-27, No.3, August, 1978.
6. A.Mosleh et al., "Procedures for Treating Common Cause Failures in Safety and Reliability Studies", NUREG/CR-4780, 1988.