A Sensitivity Study of Human Errors in Optimizing Surveillance Test Interval (STI) and Allowed Outage Time (AOT) of Standby Safety System

Dae Wook Chung and Won Ky Shin

Korea Institute of Nuclear Safety
P.O.Box 114, Yusung, Taejon, Republic of Korea
Tel) 82-42-868-0220, Fax) 82-42-861-1700,
e-mail) k156cdw@pinpoint.kins.re.kr

Young Woo You and Hui Chang Yang

Seoul National University
Shinlim-dong, Kwanak-ku, Seoul, Republic of Korea
Tel) 82-02-875-8868, Fax) 82-02-889-2688,
e-mail) changs@plaza.snu.ac.kr

Abstract

In most cases, the surveillance test intervals (STIs), allowed outage times (AOTS) and testing strategies of safety components in nuclear power plant are prescribed in plant technical specifications. And, in general, it is required that standby safety system shall be redundant (i.e., composed of multiple components) and thes components are tested by either staggered test strategy or sequential test strategy. In this study, a linear model is presented to incorporate the effects of human errors associated with test into the evaluation of unavailability. The average unavailabilities of 1/4, 2/4 redundant systems are computed considering human error and testing strategy. The adverse effects of test on system unavailability, such as component wear and test-induced transient have been modelled. The final outcome of this study would be the optimized human error domain from 3-D human error sensitivity analysis by selecting finely classified segment. The results of sensitivity analysis show that the STI and AOT can be optimized provided human error probability is maintained within allowable range.

1. Introduction

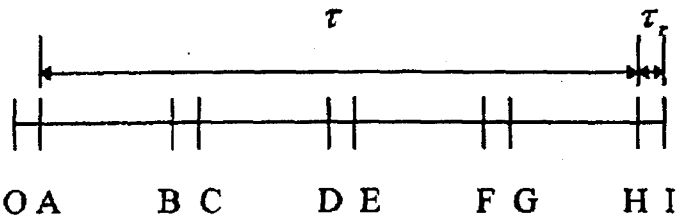
The surveillance test intervals (STIs), allowed outage times (AOTS) and testing strategies of safety components in nuclear power plant are prescribed in plant technical specifications. However, most of the existing STIs and AOTs have been determined on the basis of conservative safety analysis and engineering judgement, resulting in a number of conservative considerations. It is known, through many recent researches[1], the improvement of safety while securing operational margins can be achieved, without any configuration change, in virtue of probabilistic safety assessment (PSA).In general, it is required that standby safety system shall be redundant (i.e., composed of multiple components) and those components are tested by either staggered test strategy or sequential test strategy in order to assure system availability. The unavailabilities of 1/4, 2/4 and 3/4 systems with sequential test strategy and those of 1/3, 2/3 systems with staggered test strategy were evaluated [2],[3]. The result show that if the system logic is more complicated than 1 out of 4, the staggered test strategy would improve the system unavailability, but it causes excessive load on the operators and, consequently, the human error associated with test. Therefore, quantification of human error effects is necessary in the course of unavailability analysis to determine the optimized STI, AOT and test strategy.

In this study, a linear model is presented to incorporate the human errors associated with test and the average unavailabilities of 1/4, 2/4 redundant systems are computed considering human error and testing strategy. Although the human errors are regarded as one of the most important contributors to system unavailability, it is hard to quantify them due to the uncertainty of human behaviour. Hence, to suggest the acceptable range of human error probability for each case, the final outcome of this study would be the optimized human error domain from 3-D human error sensitivity analysis by selecting finely classified segment. For case study, the auxiliary feedwater system of Younggwang nuclear units 3&4 is selected. (2-out-of-4 system logic)

2. Application to 1/4 and 2/4 System Unavailability

2.1 Testing Strategy

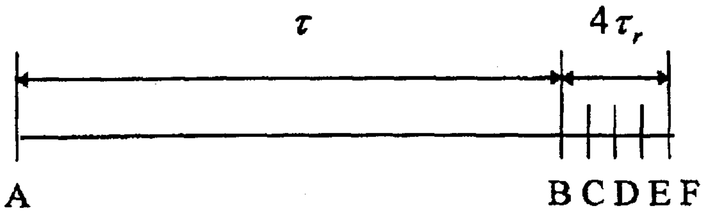
Current technical specification allows two types of testing strategy. One is the sequential test strategy by which all components are tested sequentially straight through one moment and the other is the staggered tes strategy by which each component is tested one and the other with the same time interval. The concept of each test strategy is graphically explained in Figures 1 and 2, respectively. The sequential test strategy may reduce the load on testing personnels compared to the staggered test strategy because all components are tested straight through one moment. However, the sequential test strategy may increase the system unavailability and dependency human error compared to the staggered test strategy . For that reason, the staggered surveillance test strategy is generally taken to minimize the system unavailability. By the way, if the



τ : surveillance test interval

τ_r : required time for test and maintenance (BC, DE, FG, HI)

Figure 1. Staggered Test Strategy



τ : surveillance test interval

τ_r : required time for test and maintenance (BC, DE, FG, HI)

Figure 2. Sequential Test Strategy

surveillance test interval of component in redundant system with 1/4, 2/4 system logic are relatively short, the staggered test strategy results in excessive loads on testing personnels, which increases the human error probability and the system unavailability. Hence one can easily find the test strategy combined by test interval plays great role in evaluating the human error and system unavailability.

2.2 Independent Failures and Common Cause Failures

It is common to use exponentialdistribution for modelling the independent failures such as demand failure and random failure of components. And the beta-factor model is applied to modelling the common cause failures. The subscript 1 and 2 denote the component type in the system. The sequence of testing is modelled to be circulated, that is the test of component i is followed by the test of component (i+1), regardless of testing strategy. The beta-factor model is applied for modelling the demand and random common cause failures since the system is composed of almost identical components. Mathematical expressions for independent failures and common cause failure are summarized as follows

$$\frac{\beta_{r1}}{(1-\beta_{r1})}\lambda_{r1} = \lambda_{c1} , \tag{1}$$

$$\lambda_{r1} + \lambda_{c1} = \lambda_1 , \tag{2}$$

$$\frac{\beta_{d1}}{(1-\beta_{d1})}D_{d1} = D_{c1} , \tag{3}$$

$$D_{d1} + D_{c1} = D_1 , \tag{4}$$

where λ_{r1} : independent running failure rate
λ_{c1} : common cause running failure rate
λ_1 : total running failure rate
D_{d1} : independent demand failure rate
D_{c1} : common cause demand failure rate
D_1 : total demand failure rate.

Above expressions can be rewritten for another type of component by replacing the subscript 1 with 2.

2.3. Adverse Effects of Test

Adverse effects of test are distinct depending on the characteristics of components. To evaluate the adverse effects, linear models for random failure rate and for demand failure rate are derived and applied to 1/4, 2/4 system using actual operating data:

Substantially, the adverse effects of test cannot be incorporated in the existing models for calculating system unavailability since constant failure rates are assumed regardless of surveillance test interval variation. Equations (5) and (6) show that failure rate also varies with surveillance test interval, which incorporate the adverse effects of test.

2.4 System Average Unavailability with Human Error Consideration

The mathematical expression for the unavailability of system having 1/4 and 2/4 system logic considering human error associated with test can be derived as follows. The number of human error occurrence during test is expected by following equation,

$$\text{Number of Human Error Occurrence} = {}_4C_3 + {}_4C_2 + {}_4C_1 + {}_4C_0 \,. \qquad (7)$$

Using above equation and conditional probability, the unavailability of 1/4 or 2/4 system can be derived as:

$$\begin{aligned} q_t = {} & \sum_{r=1}^{4} P_r\left\{S\middle|E_4E_3E_2E_1\right\} \prod_{k=1}^{4} P_r\left\{E_{5-k}\middle|E_{4-k}E_{3-k}E_{2-k}\right\} + \sum_{r=1}^{3}\sum_{l=r+1}^{4} P_{rl}\left\{S\middle|E_4E_3E_2E_1\right\} \\ & \times \prod_{k=1}^{4} P_{rl}\left\{E_{5-k}\middle|E_{4-k}E_{3-k}E_{2-k}\right\} + \sum_{r=1}^{2}\sum_{l=r+1}^{3}\sum_{j=l+1}^{4} P_{rlj}\left\{S\middle|E_4E_3E_2E_1\right\} \prod_{k=1}^{4} P_{rlj}\left\{E_{5-k}\middle|E_{4-k}E_{3-k}E_{2-k}\right\} \\ & + P_{1234}\left\{S\middle|E_4E_3E_2E_1\right\} \prod_{k=1}^{4} P_{1234}\left\{E_{5-k}\middle|E_{4-k}E_{3-k}E_{2-k}\right\} \,. \end{aligned} \qquad (8)$$

From equation (8), after some tedious derivation, *q(t)* can be obtained and the system average unavailability can be obtained by:

$$q_{av} = \frac{1}{T}\left[\int_A^B q(t)dt + \int_B^C q(t)dt + \int_C^D q(t)dt + \int_D^E q(t)dt + \cdots + \int_H^I q(t)dt\right]. \qquad (9)$$

As shown in Eq.(8), the system average unavailability has 15 factors and can be expressed by following equation:

$$q_{av} = \sum_{av=1}^{15} F_{av} \,. \qquad (10)$$

F_{av} can be computed using equation (8) and listed in Tables 1 and 2 by separating CCF and human error terms.

The conditional probability of a human error occurrence associated with test can be expressed as γ_0. For two successive occurrencesof human errors, it is $\gamma_0\gamma_1$, and for three successive occurrences of human errors it is $\gamma_0\gamma_1\gamma_2$, and so forth. The characteristics ofthese conditional probability probabilities in terms of dependency are as below.

Strategy

$$\lambda = \lambda_0 \left\{(1-P) + P\left(\frac{W}{T}\right)\right\} , \quad (5)$$

$$D = D_0 \left\{(1-P) + P\left(\frac{W}{T}\right)\right\} , \quad (6)$$

where λ_0 : random failure rate with reference test interval
D_0 : demand failure rate with reference test interval
T : surveillance test interval
W : reference test interval
P : wear effect ratio of test.

Ite		uential Test
F1		$+ D_{d2}D_{d1}^2) + 2(D_{c1}D_{d2} + D_{c2}D_{d1})$
F2		$\lambda_{r1})\tau + 2(D_{d1}D_{d2}\lambda_{r1} + D_{d1}D_{d2}\lambda_{r2})\tau$
F3		$\lambda_{r2}\lambda_{r1})\frac{4\tau^2}{3} + (D_{d2}\lambda_{r1}^2 + D_{d1}\lambda_{r2}^2)\frac{2\tau^2}{3}$
F4	$(\lambda_{r1}^2\lambda_{r2} + \lambda_{r1}\lambda_{r2}^2)\frac{23\tau^3}{384} + (\lambda_{c1}\lambda_{r2} + \lambda_{c2}\lambda_{r1})\frac{35\tau^2}{48}$	$(\lambda_{r1}^2\lambda_{r2} + \lambda_{r1}\lambda_{r2}^2)\frac{\tau^3}{2} + (\lambda_{c1}\lambda_{r2} + \lambda_{c2}\lambda_{r1})\frac{2\tau^2}{3}$
F5	$(D_{c1}\lambda_{r2} + D_{c2}\lambda_{r1})\tau + (D_{d2}\lambda_{c1} + D_{d1}\lambda_{c2})\frac{\tau}{2}$	$(D_{c1}\lambda_{r2} + D_{c2}\lambda_{r1})\tau + (D_{d2}\lambda_{c1} + D_{d1}\lambda_{c2})\tau$
F6	$2\{D_{d1}^2 + D_{c1} + D_{d2}^2 + D_{c2} + 2(D_2D_{d1} + D_1D_{d2})\}\frac{\tau_r}{\tau}$	$2\{D_{d1}^2 + D_{c1} + D_{d2}^2 + D_{c2} + 2(D_2D_{d1} + D_1D_{d2})\}\frac{\tau_r}{\tau}$
F7	$2(D_{d2}\lambda_{2} + D_1\lambda_{r2} + D_{d2}\lambda_1 + D_{d1}\lambda_{r1} + D_2\lambda_{r1} + D_{d1}\lambda_2)\tau_r$	$(3D_{d2}\lambda_{r2} + 3D_1\lambda_{r2} + 2D_{d2}\lambda_1 + D_{d1}\lambda_{r1} + D_2\lambda_{r1} + 2D_{d1}\lambda_2)\tau_r$
F8	$(\lambda_{c1} + \lambda_{c2})\frac{3\tau_r}{2} + (\lambda_1\lambda_{r2} + \lambda_2\lambda_{r1})\tau\tau_r$	$(\lambda_{c1} + 2\lambda_{c2})\tau_r + \left(\lambda_{r2}^2 + 2\lambda_1\lambda_{r2} + \lambda_2\lambda_{r2} + \lambda_{r1}^2\frac{\tau_r}{2\tau}\right)\tau\tau_r$

Methodologies for evaluating the human error have been continuously developed and a number of researches have been done for the application to actual situations. Nevertheless, it seems that there is no single methodology which is prevalent and generally accepted for human error evaluation. In this regard, there exists many difficulties in analysing human errors associated with nuclear power plant operation. Up to now, several methodologies such as THERP, SLIM, HCR

Mutually Dependent Case : $\gamma_0 < \gamma_1 < \gamma_2 < \gamma_3 < \cdots$ (11)

Mutually Independent Case : $\gamma_0 = \gamma_1 = \gamma_2 = \gamma_3 = \cdots .$ (12)

Table 2. The F_{av} Equations for Each Testing Strategy
(Independent Failures and Human Errors)

Item	Staggered Test	Sequential Test
F9	$2(\gamma_1\gamma_2^2+\gamma_1^2\gamma_2)+4\gamma_1\gamma_2\left\{D_t+\frac{\tau}{2}(\lambda_1+\lambda_2)\right\}$	$2(\gamma_1\gamma_2^2+\gamma_1^2\gamma_2)+4\gamma_1\gamma_2\left(D_t+\lambda_t\frac{\tau}{2}\right)$
F10	$\gamma_2^2\left\{(D_1+D_{d1})+\frac{\tau}{2}(\lambda_{r1}+\lambda_1)\right\}+\gamma_2^2\left\{(D_1+D_{d1})+\frac{\tau}{2}(\lambda_{r1}+\lambda_1)\right\}$	$\gamma_2^2\left\{(D_1+D_{d1})+\frac{\tau}{2}(\lambda_{r1}+\lambda_1)\right\}+\gamma_1^2\left\{(D_2+D_{d2})+\frac{\tau}{2}(\lambda_{r2}+\lambda_2)\right\}$
F11	$2\gamma_1\{D_{d2}^2+D_{c2}+2D_1D_{d2}+(D_{d2}\lambda_{r2}+D_{d2}\lambda_1+D_1\lambda_{r2})\tau$ $+\lambda_{c2}\frac{3\tau}{4}+\lambda_{r1}^2\frac{5\tau^2}{24}+\lambda_1\lambda_{r2}\frac{31\tau^2}{24}\ \}$	$2\gamma_1\{D_{d2}^2+D_{c2}+2D_1D_{d2}+(D_{d2}\lambda_{r2}+D_{d2}\lambda_1+D_1\lambda_{r2})\tau$ $+\lambda_{c2}\frac{\tau}{2}+\lambda_{r2}^2\frac{\tau^2}{3}+\lambda_2\lambda_{r1}\frac{2\tau^2}{3}\ \}$
F12	$2\gamma_2\{D_{d1}^2+D_{c1}+2D_2D_{d1}+(D_{d1}\lambda_{r1}+D_{d1}\lambda_2+D_2\lambda_{r1})\tau$ $+\lambda_{c1}\frac{3\tau}{4}+\lambda_{r1}^2\frac{5\tau^2}{24}+\lambda_2\lambda_{r1}\frac{31\tau^2}{24}\ \}$	$2\gamma_2\{D_{d1}^2+D_{c1}+2D_2D_{d1}+(D_{d1}\lambda_{r1}+D_{d1}\lambda_2+D_2\lambda_{r1})\tau$ $+\lambda_{c1}\frac{\tau}{2}+\lambda_{r1}^2\frac{\tau^2}{3}+\lambda_2\lambda_{r1}\frac{2\tau^2}{3}\ \}$
F13	$2(4\gamma_1\gamma_2+\gamma_1^2+\gamma_2^2)\frac{\tau_r}{\tau}$	$2(4\gamma_1\gamma_2+\gamma_1^2+\gamma_2^2)\frac{\tau_r}{\tau}$
F14	$2\gamma_1\left\{(D_2+D_{d2})\frac{\tau_r}{\tau}+\lambda_2\frac{3\tau_r}{4}+\lambda_{r2}\frac{\tau_r}{4}+2D_t\frac{\tau_r}{\tau}+\lambda_t\tau_r\right\}$	$2\gamma_1\left\{(D_2+D_{d2})\frac{\tau_r}{\tau}+\lambda_2\frac{3\tau_r}{2}+\lambda_{r2}\frac{\tau_r}{2}+2D_t\frac{\tau_r}{\tau}+\lambda_t\frac{\tau_r}{2}\right\}$
F15	$2\gamma_2\left\{(D_1+D_{d1})\frac{\tau_r}{\tau}+\lambda_1\frac{3\tau_r}{4}+\lambda_{r1}\frac{\tau_r}{4}+2D_t\frac{\tau_r}{\tau}+\lambda_t\tau_r\right\}$	$2\gamma_2\left\{(D_1+D_{d1})\frac{\tau_r}{\tau}+2D_t\frac{\tau_r}{\tau}+\lambda_t\frac{3\tau_r}{2}\right\}$

and ASEP which is shortened form of THERP, have been regarded as appropriate to some extent. Except HCR, it is thought any methodology can be applicable to STI/AOT evaluation so long as it is related to pre-accident human error analysis. However, it is recommendable to select appropriate methodology for specific system depending on the characteristic of the system.

The scope of this study is limited to the evaluation of pre-accidents human error (human errors during test and maintenance), and the conditional probability concept is applied based on THERP methodology. In Summary

1) Types of Human Error Associated with Test and Maintenance

- Error of Commission (ECOM): Human Error During Commissioning the Test and Maintenance tasks,
- Error of Omission (EOM): Human Error of Omitting the Restoration of System After Test and Maintenance Tasks.

2) Probability Used Depending on the Dependency of Human Error

- Zero Dependency: HEP,
- Medium Dependency:(1+6XHEP)/7. (13)

In this study, sensitivity analysis of the human error is performed by treating both ECOM and EOM collectively and henceforth through entiresensitivity analysis, the probability of human error would be the sum of both type human error probabilities.

The human error dependency on the testing strategy are summarized as below

1) For Staggered Testing Strategy:Mutually Independent,
2) For Sequential Testing Strategy:Medium Dependency.

3. Human Error Sensitivity Analysis to STI/AOT

3.1 Human Error Sensitivity Analysis to Surveillance Test Interval

In previous chapter, the average system unavailability of 1/4, 2/4 redundant system is derived using failure probabilities and test parameters for each testing strategy, and the key results are summarized in Tables 1 and 2. However, as previously mentioned, there are somedifficulties in quantifying the human error probability for use in evaluating STI/AOT. Thus, it is judged that sensitivity analysis of human error can give more useful results and insight related to effect of human error. on the evaluation. of STI/AOT. Various human error sensitivity analyses was performed for auxiliary feedwater system (AFWS) of Younggwang nuclear units 3&4 with system logic of 2-out-of-4.

As shown in Figure 3, the AFWS is composed of two trains and each train is equipped one motor-driven pump and one diesel-driven pump. The quantitative value of component failure probability, common cause failure probability, and the range of human error probability of concern is presented in Table 3. The applied range of human error probability in this analysis is set for covering the whole HEP range used in PSA.

Applying the equations in Tables 1 and 2 and the failure data in Table 3, the human error sensitivity analyses to surveillance test interval were performed and the results are shown in Figures 4 and 5 for each testing strategy. As shown in Figures, five domains can be identified according to the unavailability range and the lowest is the optimized domain of human error in terms of unavailability. Current surveillance test interval is set as 30 days and staggered testing

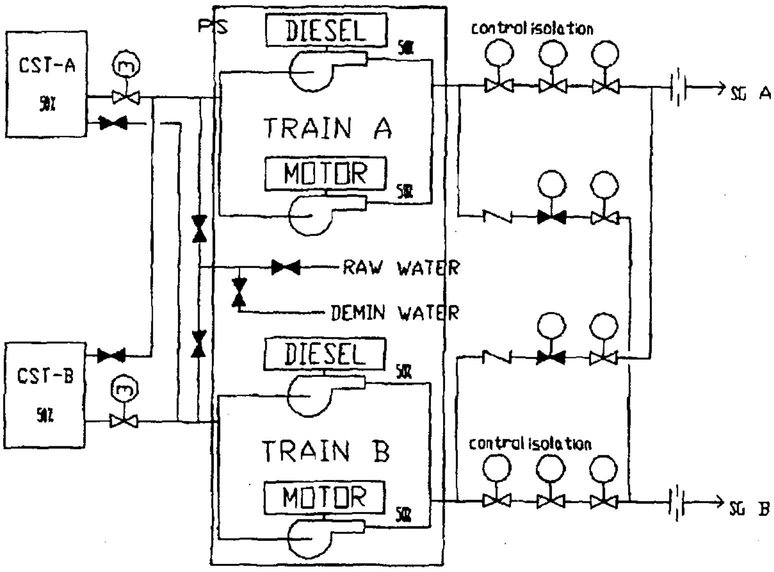


Figure 3. Simplified P&ID of YGN 3&4 AFWS

Table 3. Failure Data of AFWS Pump by Failure Modes

	Demand Failure Rate	Demand Failure Rate	CCCF(Beta)	HEP Range	AOT
Motor Driven Pump	3.0E-3/d	1.5E-4/hr	1.0546 (fail to start) 0.003 (fail to run)	0.1 ~ 0.0001	2 hr
Diesel Driven Pump	2.0E-2/d	1.0E-4/hr	0.0546 (fail to start) 0.003 (fail to run)	0.1 ~ 0.0001	2 hr

Table 4. Distribution of AFWS Pump Failure Causes

LACK of Lubrication or Cooling	Maintenance Error	Wear/End of Life	Not Stated	Etc.
23 %	17 %	15 %	19 %	23 %

strategy is applied. It can be easily found from Figure 4, the maximum allowable HEP is 0.07 with current surveillance test interval, however, it is 0.03 with the surveillance test interval of 90 days. This results suggest one of the important interpretations that once the probability of human error is maintained at low level, the STI can be relaxed without any impact on system unavailability. For sequential testing strategy case, as shown in Figure 5, because of high dependency of human error and high common cause failure probability, the maximum allowable HEP is 0.03 with the surveillance test interval of 50 days. System unavailability varies rapidly with human error probability in the domain next to optimized domain, which means that the optimization can not be applied in this domain for the AFWS, but can be applied for those system of less contribution to plant safety. Remaining 3 domains are regarded as inappropriate in any case. Thus, this type of sensitivity analysis can be used in balancing the STI and HEP, and in optimizing the STI by providing allowable HEP range.

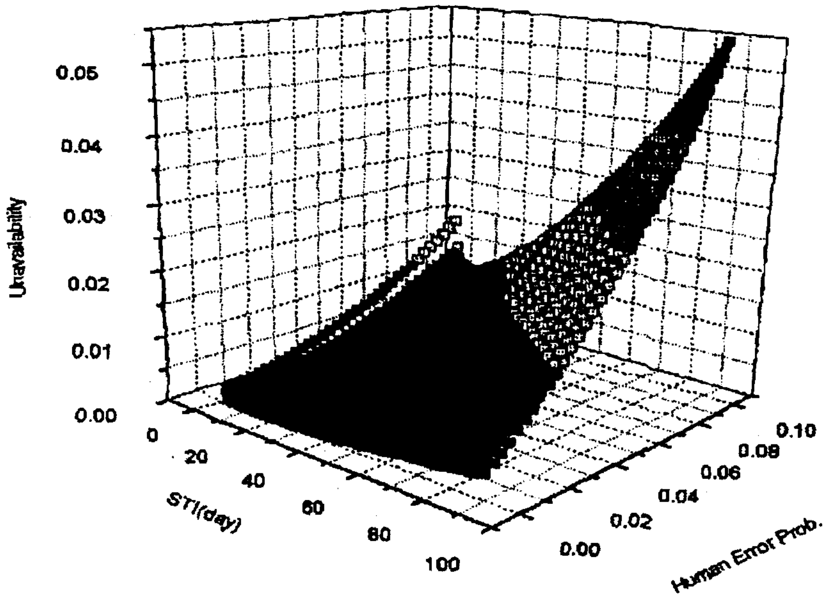


Figure 4. Human Error Sensitivity Analysis for Staggered Test Strategy Case

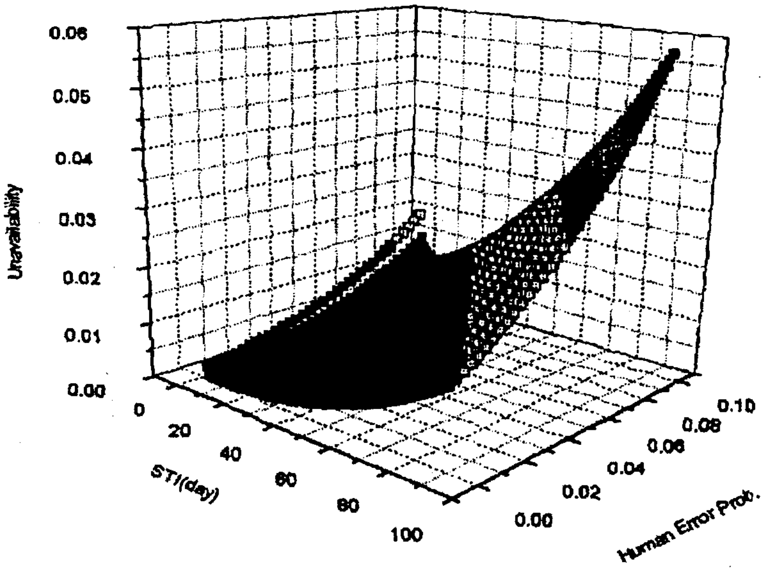


Figure 5. Human Error Sensitivity Analysis for Sequential Test Strategy case

3.2 Human Error Sensitivity Analysis to Allowed Outage Time

The standby safety system becomes unavailable when it is tested and/or subject to maintenance and the time duration for the test and maintenance is regarded as the allowed outage time (AOT). The effect of AOT on system unavailability is shown to be relatively small in case that human error is not incorporated in the optimization process. However, recently the human error aspect is regarded as one of the major contributor to system unavailability and it is noted that all the human errors occur within the AOT. Thus, human error sensitivity analysis to AOT was performed to provide the allowable domain of HEP with respect to AOT ranged from 0 to 24 hrs.

Figures 6 and 7 shows the sensitivity analysis results to human error and allowed outage time with the surveillance test interval of 30 days and 90 days, respectively. Similar to the STI case, five domains are identified according to the unavailability range, and the two lowest domain is applicable to the optimization. The results in Figure 6 show that the effect of human error varies more sensitively than that in Figure 7, but the change in unavailability is still negligible in both cases even though the human error is considered.

4.Conclusion

The applicable range of human error probability is determined through various sensitivity analysis of human error with a view to optimizing the surveillance test interval (STI) and allowed outage time (AOT) of components in redundant safety system. For actual calculation, auxiliary feedwater system is selected and the results show that the STI and AOT can be optimized provided human error probability is maintained within allowable range. This conclusion can be expanded to other system if the characteristics of system is well reflected.

5. References

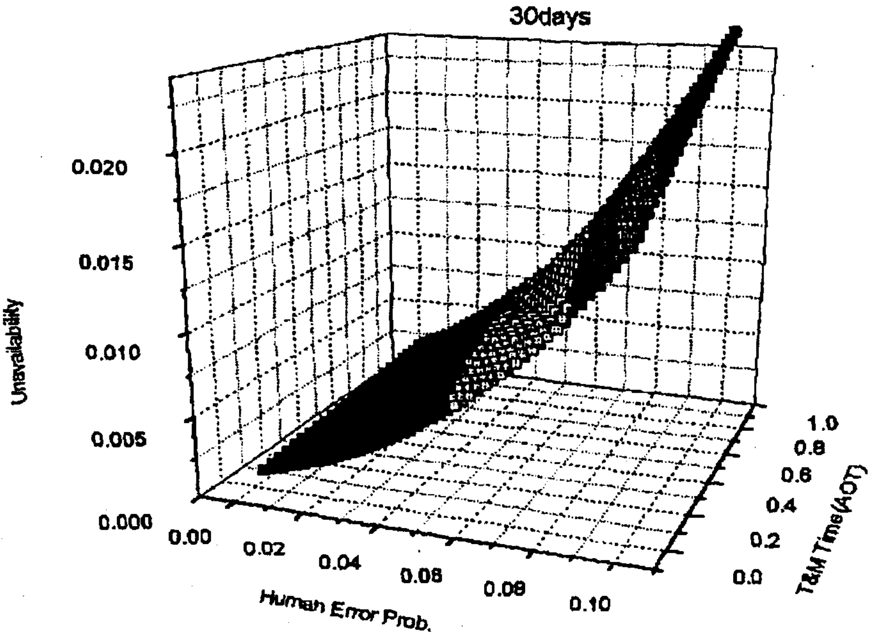


Figure 6. Human Error and T&M Time (AOT) Sensitivity Analysis For Staggered Test Strategy

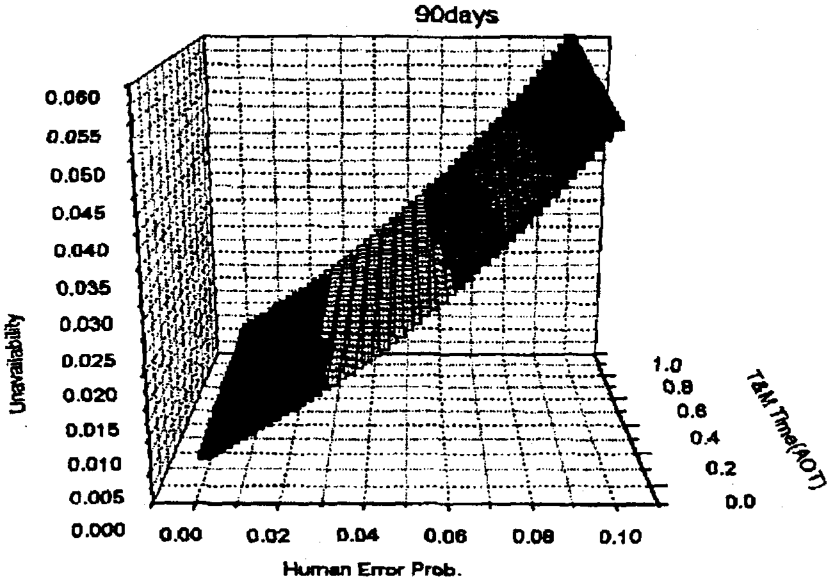


Figure 7. Human Error and T&M Time(AOT) Sensitivity Analysis for Sequential Test Strategy

[1] Lobel R. and Tjader T. R.,"Improvements to Technical Specification Surveillance Requirement, "NUREG-1 366, May 1992

[2] G. E. Apostolakis and P. P. Bansal,"Effect of Human Error on the Unavailability of Periodically Inspected Redundant Systems," IEEE Trans. Reliab. R-26, 220, 1977

[31 G. E. Apostolakis and T. L. Chu,"The Unavailability of Systems under Periodic Test and Maintenance," Nuclear Technology, vol. 50, 1980

[4] US NRC, "Standard Technical Specifications," NUREG-1432, Oct. 1992

[5] A. D. Swain, "HRA Handbook," NUREG/CR-1278

[6] KAERI, "Final Level IPRA for Younggwang Nuclear Unit 3 and 4," July 1993

[7] M. L. Adams and E. Makay, "Aging and Service Wear of Auxiliary Feedwater Pumps for PWR Nuclear Power Plants," NUREG/CR-4597, July 1986