*Journal of the Korean Nuclear Society*
*Volume 26, Number 1, March 1994*

# Optimal Inspection Periods of Safety System of Wolsung Nuclear Power Plant Unit 1 with Human Error Consideration

**Jin Il Mok and Poong Hyun Seong**
Korea Advanced Institute of Science and Technology
(Received August 3, 1993)

# 인간실수를 고려한 월성 원자력발전소 안전계통의 최적점검주기에 관한 연구

**목진일 · 성풍현**
한국과학기술원
(1993. 8. 3 접수)

## Abstract

The engineered safeguards of Wolsung nuclear power plant unit 1 contain redundant systems of 2-out-of-3 logic which are not operating under normal conditions but are called upon to act when emergency conditions develop. To ensure their operability, the systems are periodically tested. In this work, we develop the unavailability formulae for 2-out-of-3 logic configurations which take into account the failure probability of the channels tested due to human error in the simultaneous testing scheme. We also develop the model for the probability that the reactor is tripped during the surveillance test due to either system failure or human error. We determined the optimal inspection periods of safety systems, taking into account both the unavailability of the safety system and the probability that the reactor is tripped during the surveillance test. We compared the results with the inspection periods currently used at Wolsung NPP Unit 1. As a result, the inspection periods obtained using a minimum human error ($8.24 \times 10^{-6}$) are shorter than those currently used in Wolsung NPP unit 1 whereas the inspection periods obtained using a maximum human error are ($4.44 \times 10^{-4}$) longer than those used in Wolsung NPP unit 1.

## 요 약

월성 원자력발전소의 안전계통은 비상사태시에만 작동하는 3분의 2논리로 구성되어 있 다. 그들의 작동성을 보증하기 위해 이 안전계통은 주기적으로 점검되어진다. 본연구에서 사람의 실수가 고려되어진 3분의 2논리 구성 시스템에서의 불이용도가 계산되어졌다. 그리고 우리는 시 험기간중에 사람의 실수또는 기계의 고장으로 인해 발전정지를 일으킬 확률을 구했다. 우리는 이 불이용도와 발전정지를 일으킬 확률을 둘다 고려하여 적정한 최적점검주기를 계산하였다. 이렇게 얻어진 점검주기와 현재 사용되는 점검주기를 비교하면, 사람의 실수를 최소($8.24 \times 10^{-6}$)로 보았을때 최

적점검주기는 현재사용되는 점검주기 보다 조금 짧았고 사람의 실 수를 최대($4.44 \times 10^{-4}$)로 보았을 때 최적점검주기는 현재 사용하는 점검 주기보다 다소 긴 것으로 계산되어 졌다.

## I. Introduction

The safety systems of Wolsung NPP unit 1 contain redundant systems of 2-out-of-3 logic[1], which are the preferred system for tripping the reactor when specified parameter exceed their operation limit. Programmable Digital Comparator are used to select the trip setpoint to compare the process signal with the setpoint and to initiate a trip if required. The trip logic of safety shutdown system employs a triplicated channel system labelled D, E and F. These channels are independent of each other. If more than two of three channels generate trip signals, the reactor is tripped. The safety system is activated by the trip parameters. The trip parameter is divided into two classes. One is the absolute trip parameter, the other is the process trip parameter. The absolute trip parameter is the one by which the trip is not determined by the Programmable Digital Comparator (PDC) but on an electronic circuit board which generates the trip signal regardless of the other trip parameters. The trip set-points of these absolute trip parameters are values which are determined absolutely regardless of the external states. The process trip parameter is the one by which the trip is determined by the PDC. The PDC determines a trip according to the present condition of NPP. Therefore, the trip set-point of the process trip parameter varies according to the present condition of the NPP. The safety systems are divided into two parts. One is the shutdown system 1 which trips the reactor by control rod. the other is the shutdown system 2 which trips the reactor by injection of gadolinium nitrate into coolant. If the shutdown system 1 does not operate when emergency condition develops, the shutdown system 2 is supposed to operate immediately. That is, the shutdown system 2 operates in case the shutdown system 1 does not operate at emergency conditions. The safety systems are activated when emergency conditions exist and their functions are to mitigate the consequences of these abnormal occurrences. Therefore the systems are to be inspected at regular intervals in order to ensure their high availability. In this work, unavailability formulae for 2-out-of-3 logic configurations are developed, taking into account of the human error in the simultaneous testing scheme (e.g., when the testing of channel is finished, channel is yet left in testing condition due to human errors). Many assumptions and the modelings in this work are quoted from Apostolakis et al [2],[3] and these are described in the following chapter.

## 2. Modeling of the Optimal Inspection Period of the Safety System

The assumptions used in modeling the optimal inspection period of the safety system are as follows[2],[3] :

1) The systems are k-out-of n : G logic configurations, i.e. system of n components is good i.f.f.(i.e. if and only if) at least k components are good.
2) The components of the system are i.i.d.(i.e. identically independent distribution) with constant failure rate $\lambda$.
3) The components of the system are sequentially inspected over a time interval $n\tau_{ts}$.
4) The time interval between completion of an inspection of all the components and initiation of the next inspection sequence is called the test (or inspection) interval and is denoted by $\tau$.

5) The period of the inspection scheme is $T = \tau + n\,\tau_{ts}$. The first period starts when the system is new and all its components are up.
6) After the completion of an inspection (at the end of the interval $\tau_{ts}$) the inspected component might not be good as new because of faulty inspection or repair, oversight, etc. These human errors can be generally classified as error of omission or commission. All these errors result in complete failures of the components or component function.
7) The probability of a component's emerging from an inspection in the failed state due to human error depends on the number of consecutive components which have gone through the tests immediately prior to the inspection of the component under consideration. The probabilities $\gamma_j$, j = 0, 1, ....., (n–1) do not depend on the period, i.e. they are the same for any two periods[4]. Thus, the operator does not improve or worsen his performance from period to period. In support of this assumption, we cite the observation made in [5] that human actions which are greatly separated in time tend to be statistical independent. Because we consider that the test interval is much longer than the testing time of the inspection. The constancy of $\gamma_j$ can be assumed.
8) The mean time to failure for each component is much longer than the period, that is,

$$T << \frac{1}{\lambda} \tag{2.1}$$

Consequently, the cumulative density function of each component for the times of interest is

$$F(t) = 1 - \exp(-\lambda t) \approx \lambda t \tag{2.2}$$

9) The (pointwise) unavailability Q(t) is the probability that the system is down at time t.
10) The probability Pr(t) is that the reactor is tripped due to human error or due to the failure of components.
11) The average system unavailability during the time interval T is defined as

$$q = \frac{\int_0^T Q(t)dt}{T} \tag{2.3}$$

and it is the proportion of the time the system is down during T (fractional dead time)[6],[7]. Eq. (2.3) is expanded to

$$q = \frac{1}{T}[\int_0^{\tau} Q(t)dt + \int_{\tau}^{\tau+\tau_{ts}} Q(t)dt + \cdots\cdots + \int_{\tau+(n-1)\tau_{ts}}^{\tau+n\tau_{ts}} Q(t)dt] \tag{2.4}$$

because Q(t) is different in each interval.
12) The average probability of inadvertent reactor trip during the time interval T is defined as

$$P_{av} = \frac{\int_0^T P(t)dt}{T} \tag{2.5}$$

Eq. (2.5) is expanded to

$$P_{av} = \frac{1}{T}[\int_0^{\tau} P(t)dt + \int_{\tau}^{\tau+\tau_{ts}} P(t)dt + \cdots\cdots + \int_{\tau+(n-1)\tau_{ts}}^{\tau+n\tau_{ts}} P(t)dt] \tag{2.6}$$

because P(t) is different in each interval.
13) Simple results are obtained from Eq. (2.2) if we use the fact that in real application the total inspection and the repairing time in each period is much shorter than the test interval, i.e.

$$n\tau_{ts} << \tau \tag{2.7}$$

Using Eq. (2.7), we write Eq. (2.4) and Eq. (2.6) as follows, respectively :

$$q \approx \frac{1}{\tau}[\int_0^{\tau} Q(t)dt + \int_{\tau}^{\tau+\tau_{ts}} Q(t)dt + \cdots\cdots + \int_{\tau+(n-1)\tau_{ts}}^{\tau+n\tau_{ts}} Q(t)dt] \tag{2.8}$$

and

$$P_{av} \approx \frac{1}{\tau}[\int_0^{\tau} P(t)dt + \int_{\tau}^{\tau+\tau_{ts}} P(t)dt + \cdots\cdots + \int_{\tau+(n-1)\tau_{ts}}^{\tau+n\tau_{ts}} P(t)dt] \tag{2.9}$$

Eq. (2.8) and Eq. (2.9) will be used to evaluate the average system unavailability and average probability of inadvertent reator trip in this paper, respectively.

### 2.1. Average Unavailability

We derive the average unavailability of a 2–out–of–3 : G system; 't=0' at the end of a sequence of renewal time (point D' in Fig. 2.1). The contribution of the average unavailability of the system from each interval D'A, AB, BC, CD is calculated and then added to yield the average unavailability of the system.

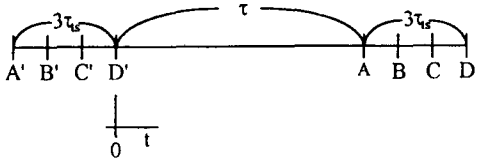


**Fig. 2.1. Simultaneous Testing Scheme for a 2–out–of–3 :**

1) During D'A ($0 \le t \le \tau$)

Define the events as follows :

Then we have the following equations :

$$\begin{aligned}
&\Pr\{\textit{system down at } t\} \\
&= \Pr\{\textit{system down at } t|E_3E_2E_1\}\Pr\{E_3|E_2E_1\}\Pr\{E_2|E_1\}\Pr\{E_1\} \\
&+\Pr\{\textit{system down at } t|\bar{E}_3E_2E_1\}\Pr\{\bar{E}_3|E_2E_1\}\Pr\{E_2|E_1\}\Pr\{E_1\} \\
&+\Pr\{\textit{system down at } t|E_3\bar{E}_2E_1\}\Pr\{E_3|\bar{E}_2E_1\}\Pr\{\bar{E}_2|E_1\}\Pr\{E_1\} \\
&+\Pr\{\textit{system down at } t|\bar{E}_3\bar{E}_2E_1\}\Pr\{\bar{E}_3|\bar{E}_2E_1\}\Pr\{\bar{E}_2|E_1\}\Pr\{E_1\} \\
&+\Pr\{\textit{system down at } t|E_3E_2\bar{E}_1\}\Pr\{E_3|E_2\bar{E}_1\}\Pr\{E_2|\bar{E}_1\}\Pr\{\bar{E}_1\} \\
&+\Pr\{\textit{system down at } t|\bar{E}_3E_2\bar{E}_1\}\Pr\{\bar{E}_3|E_2\bar{E}_1\}\Pr\{E_2|\bar{E}_1\}\Pr\{\bar{E}_1\} \\
&+\Pr\{\textit{system down at } t|E_3\bar{E}_2\bar{E}_1\}\Pr\{E_3|\bar{E}_2\bar{E}_1\}\Pr\{\bar{E}_2|\bar{E}_1\}\Pr\{\bar{E}_1\} \\
&+\Pr\{\textit{system down at } t|\bar{E}_3\bar{E}_2\bar{E}_1\}\Pr\{\bar{E}_3|\bar{E}_2\bar{E}_1\}\Pr\{\bar{E}_2|\bar{E}_1\}\Pr\{\bar{E}_1\}. \quad (2.10)
\end{aligned}$$

$$\begin{aligned}
&\Pr\{\textit{system down at } t|E_3E_2E_1\} = \Pr\{\textit{system down at } t|\bar{E}_3E_2E_1\} \\
&= \Pr\{\textit{system down at } t|E_3\bar{E}_2E_1\} = \Pr\{\textit{system down at } t|E_3E_2\bar{E}_1\} = 1, \\
&\Pr\{\textit{system down at } t|\bar{E}_3\bar{E}_2E_1\} = F(t+\tau_{ts}) + F(t) = \lambda(t+\tau_{ts}) + \lambda(t), \\
&\Pr\{\textit{system down at } t|\bar{E}_3E_2\bar{E}_1\} = F(t+2\tau_{ts}) + F(t) = \lambda(t+2\tau_{ts}) + \lambda(t), \\
&\Pr\{\textit{system down at } t|E_3\bar{E}_2\bar{E}_1\} = F(t+2\tau_{ts}) + F(t+\tau_{ts}) \\
&\qquad = \lambda(t+2\tau_{ts}) + \lambda(t+\tau_{ts}), \\
&\Pr\{\textit{system down at } t|\bar{E}_3\bar{E}_2\bar{E}_1\} = F(t+\tau_{ts})F(t) + F(t+\tau_{ts})F(t+2\tau_{ts}) \\
&\qquad +F(t+2\tau_{ts})F(t) \\
&\qquad = \lambda^2(t+\tau_{ts})t + \lambda^2(t+\tau_{ts})(t+2\tau_{ts}) \\
&\qquad +\lambda^2(t+2\tau_{ts})t.
\end{aligned}$$

Eq. (2.10) is then rewritten as

$$\begin{aligned}
Q_{D'A}(t) &= \gamma_2\gamma_1\gamma_0 + (1-\gamma_2)\gamma_1\gamma_0 + \gamma_0(1-\gamma_1)\gamma_0 + \gamma_1\gamma_0(1-\gamma_0) \\
&+[\lambda(t+\tau_{ts}) + \lambda t](1-\gamma_0)(1-\gamma_1)\gamma_0 + [\lambda(t+2\tau_{ts}) \\
&+\lambda t)](1-\gamma_0)(1-\gamma_1)\gamma_0 \\
&+[\lambda(t+\tau_{ts}) + \lambda(t+2\tau_{ts})](1-\gamma_0)^2\gamma_0 \\
&+[\lambda^2(t+\tau_{ts})t + \lambda^2(t+2\tau_{ts})(t+\tau_{ts}) \\
&+\lambda^2(t+2\tau_{ts})t](1-\gamma_0)^3. \qquad (2.11)
\end{aligned}$$

The contribution to the average unavailability from D'A, i.e., the first term on the r.h.s of Eq. (2.8), is

$$\begin{aligned}
q_{D'A} &= \frac{\int_0^\tau Q_{D'A}(t)dt}{\tau} = \gamma_0(2\gamma_1 + \gamma_0 - \gamma_0^2 - \gamma_1\gamma_0) \\
&+(1-\gamma_0)(1-\gamma_1)\gamma_0\lambda(2\tau+3\tau_{ts}) + (1-\gamma_0)^2\gamma_0\lambda(\tau+3\tau_{ts}) \\
&+(1-\gamma_0)^3\lambda^2(\tau^2+3\tau_{ts}\tau+2\tau_{ts}^2). \qquad (2.12)
\end{aligned}$$

2) During AB ($\tau \le t \le \tau + \tau_{ts}$)

During the interval AB one of the channels is inspected and the unavailability of channel being inspected is unity. Therefore, this system is equal to 2–out–of–2 logic system during the inspection time. Its expression is derived using arguments similar to the ones that led to Eq. (2.11). We have the following equations :

$$\begin{aligned}
&\Pr\{\textit{system down at } t\} \\
&= \Pr\{\textit{system down at } t|E_3E_2E_1\}\Pr\{E_3|E_2E_1\}\Pr\{E_2|E_1\}\Pr\{E_1\} \\
&+\Pr\{\textit{system down at } t|\bar{E}_3E_2E_1\}\Pr\{\bar{E}_3|E_2E_1\}\Pr\{E_2|E_1\}\Pr\{E_1\} \\
&+\Pr\{\textit{system down at } t|E_3\bar{E}_2E_1\}\Pr\{E_3|\bar{E}_2E_1\}\Pr\{\bar{E}_2|E_1\}\Pr\{E_1\} \\
&+\Pr\{\textit{system down at } t|\bar{E}_3\bar{E}_2E_1\}\Pr\{\bar{E}_3|\bar{E}_2E_1\}\Pr\{\bar{E}_2|E_1\}\Pr\{E_1\} \\
&+\Pr\{\textit{system down at } t|E_3E_2\bar{E}_1\}\Pr\{E_3|E_2\bar{E}_1\}\Pr\{E_2|\bar{E}_1\}\Pr\{\bar{E}_1\} \\
&+\Pr\{\textit{system down at } t|\bar{E}_3E_2\bar{E}_1\}\Pr\{\bar{E}_3|E_2\bar{E}_1\}\Pr\{E_2|\bar{E}_1\}\Pr\{\bar{E}_1\} \\
&+\Pr\{\textit{system down at } t|E_3\bar{E}_2\bar{E}_1\}\Pr\{E_3|\bar{E}_2\bar{E}_1\}\Pr\{\bar{E}_2|\bar{E}_1\}\Pr\{\bar{E}_1\} \\
&+\Pr\{\textit{system down at } t|\bar{E}_3\bar{E}_2\bar{E}_1\}\Pr\{\bar{E}_3|\bar{E}_2\bar{E}_1\}\Pr\{\bar{E}_2|\bar{E}_1\}\Pr\{\bar{E}_1\} \quad (2.13)
\end{aligned}$$

$$\begin{aligned}
&\Pr\{\textit{system down at } t|E_3E_2E_1\} = \Pr\{\textit{system down at } t|E_3E_2\bar{E}_1\} = 1 \\
&\Pr\{\textit{system down at } t|\bar{E}_3E_2E_1\} = \Pr\{\textit{system down at } t|\bar{E}_3E_2\bar{E}_1\} = F(t) = \lambda(t) \\
&\Pr\{\textit{system down at } t|E_3\bar{E}_2E_1\} = \Pr\{\textit{system down at } t|E_3\bar{E}_2\bar{E}_1\} \\
&\qquad = F(t+\tau_{ts}) = \lambda(t+\tau_{ts}) \\
&\Pr\{\textit{system down at } t|\bar{E}_3\bar{E}_2E_1\} = \Pr\{\textit{system down at } t|\bar{E}_3\bar{E}_2\bar{E}_1\} \\
&\qquad = F(t)F(t+\tau_{ts}) = \lambda^2 t(t+\tau_{ts})
\end{aligned}$$

Eq. (2.13) is written as

$$\begin{aligned}
Q_{AB}(t) &= \gamma_2\gamma_1\gamma_0 + \lambda t(1-\gamma_2)\gamma_1\gamma_0 + \lambda(t+\tau_{ts})\gamma_0^2(1-\gamma_0) + \gamma_1\gamma_0(1-\gamma_0) \\
&+\lambda^2 t(t+\tau_{ts})(1-\gamma_0)(1-\gamma_1)\gamma_0 + \lambda t(1-\gamma_0)(1-\gamma_1)\gamma_0 \\
&+\lambda(t+\tau_{ts})(1-\gamma_0)^2\gamma_0 + \lambda^2 t(t+\tau_{ts})(1-\gamma_0)^3 \qquad (2.14)
\end{aligned}$$

The contribution to the average unavailability from AB, i.e., the second term on the r.h.s of Eq. (2.8), is

$$q_{AB} = \frac{\int_{\tau}^{\tau+\tau_{is}} Q_{AB}(t)dt}{\tau}$$

$$= \frac{1}{\tau}\Big\{\tau_{is}\gamma_0\gamma_1(1-\gamma_0+\gamma_2) + \lambda\tau_{is}^2[\gamma_0^2(1-\gamma_1)+\gamma_0(1-\gamma_0)^2] + \frac{\lambda[(\tau+\tau_{is})^2-\tau^2]}{2}$$

$$[(1-\gamma_2)\gamma_1\gamma_0+\gamma_0(1-\gamma_1)+\gamma_0^2(1-\gamma_1)^2+\lambda\tau_{is}(1-\gamma_0)[\gamma_0(1-\gamma_1)+(1-\gamma_0)^2]]$$

$$+\frac{\lambda^2}{3}(1-\gamma_0)[\gamma_0(1-\gamma_1)+(1-\gamma_0)^2][(\tau+\tau_{is})^3+\tau^3]\Big\} \qquad (2.15)$$

3) During BC $(\tau+\tau_{is} \le t \le \tau+2\tau_{is})$

During the interval BC one of the channels is inspected and unavailability of channel being inspected is unity. Therefore, this system is equal to 2–out–of–2 logic system during the inspection time. Its expression is derived using arguments similar to the ones that led to Eq. (2.14). We have the following equations :

$$\Pr\{\textit{system down at } t|E_3E_2E_1\} = \Pr\{\textit{system down at } t|\bar{E}_3E_2E_1\}$$
$$= \Pr\{\textit{system down at } t|E_3E_2\bar{E}_1\} = \Pr\{\textit{system down at } t|E_3\bar{E}_2\bar{E}_1\}$$
$$= F(t-\tau-\tau_{is}) = \lambda(t-\tau-\tau_{is})$$
$$\Pr\{\textit{system down at } t|\bar{E}_3E_2E_1\} = \Pr\{\textit{system down at } t|\bar{E}_3\bar{E}_2E_1\}$$
$$= \Pr\{\textit{system down at } t|\bar{E}_3E_2\bar{E}_1\} = \Pr\{\textit{system down at } t|\bar{E}_3\bar{E}_2\bar{E}_1\}$$
$$= F(t-\tau-\tau_{ys})F(t+\tau_{is}) = \lambda^2(t-\tau-\tau_{is})(t+\tau_{is})$$

Unavailability during BC is written as

$$Q_{BC}(t) = \lambda(t-\tau-\tau_{is})[\gamma_2\gamma_1\gamma_0+\gamma_0^2(1-\gamma_0)+\gamma_1\gamma_0(1-\gamma_0)+\gamma_0(1-\gamma_0)^2]$$
$$+\lambda^2\tau_{is}(t^2-\pi-\tau\tau_{is}-\tau_{is}^2)[\gamma_0\gamma_1(1-\gamma_2)+2\gamma_0(1-\gamma_0)$$
$$(1-\gamma_1)+(1-\gamma_0)^3] \qquad (2.16)$$

The contribution to the average unavailability from BC, i.e., the second term on the r.h.s of Eq. (2.8), is

$$q_{BC} = \frac{\int_{\tau+\tau_{is}}^{\tau+2\tau_{is}} Q_{BC}(t)dt}{\tau}$$

$$= \frac{1}{\tau}\Big\{\lambda\tau_{is}^2[\gamma_2\gamma_0\gamma_1+\gamma_0^2(1-\gamma_1)+\gamma_0\gamma_1(1+\gamma_0)+\gamma_0(1+\gamma_0)^2]$$

$$\times[\frac{1}{2}((\tau+2\tau_{is})^2-(\tau+\tau_{is})^2)-(\tau+\tau_{is})\tau_{is}]$$

$$+\lambda^2[\gamma_0\gamma_1(1-\gamma_2)+2\gamma_0(1-\gamma_0)(1-\gamma_1)+(1-\gamma_0)^3]$$

$$\times[\frac{1}{3}((\tau+2\tau_{is})^3-(\tau+\tau_{is})^3)-\frac{\tau}{2}((\tau+2\tau_{is})^2-(\tau+\tau_{is})^2)$$

$$-\tau_{is}^2(\tau+\tau_{is})]\Big\} \qquad (2.17)$$

4) During CD $(\tau+2\tau_{is} \le t \le \tau+3\tau_{is})$

During the interval CD one of the channels is inspected and unavailability of channel being inspected is unity. Therefore, this system is equal to 2–out–of–2 logic system during the inspection time. We have the following equations :

$$\Pr\{\textit{system down at } t|E_3E_2E_1\} = \Pr\{\textit{system down at } t|E_3\bar{E}_2E_1\}$$
$$= \Pr\{\textit{system down at } t|E_3E_2\bar{E}_1\} = \Pr\{\textit{system down at } t|E_3\bar{E}_2\bar{E}_1\}$$
$$= \Pr\{\textit{system down at } t|\bar{E}_3E_2E_1\} = \Pr\{\textit{system down at } t|\bar{E}_3\bar{E}_2E_1\}$$
$$= \Pr\{\textit{system down at } t|\bar{E}_3E_2\bar{E}_1\} = \Pr\{\textit{system down at } t|\bar{E}_3\bar{E}_2\bar{E}_1\}$$
$$= F(t-\tau-\tau_{ys})F(t-\tau-2\tau_{is}) = \lambda^2(t-\tau-\tau_{is})(t-\tau-2\tau_{is}).$$

Unavailability during CD is written as

$$Q_{CD}(t) = \lambda^2(t-\tau-\tau_{is})(t-\tau-2\tau_{is})[\gamma_2\gamma_1\gamma_0+\gamma_0\gamma_1(1-\gamma_2)+\gamma_0^2(1-\gamma_1)$$
$$+\gamma_0(1-\gamma_0)(1-\gamma_1)+\gamma_0\gamma_1(1-\gamma_0)+\gamma_0(1-\gamma_0)(1-\gamma_1)$$
$$+\gamma_0(1-\gamma_0)^2+(1-\gamma_0)^3]. \qquad (2.18)$$

The contribution to the average unavailability from CD, i.e., the fourth term on the r.h.s of Eq. (2.8), is

$$q_{CD} = \frac{\int_{\tau+2\tau_{is}}^{\tau+3\tau_{is}} Q_{CD}(t)dt}{\tau}$$

$$= \frac{1}{\tau}\Big\{\lambda^2[\gamma_2\gamma_1\gamma_0+\gamma_0\gamma_1(1-\gamma_2)+\gamma_0^2(1-\gamma_1)+\gamma_0(1-\gamma_0)(1-\gamma_1)$$
$$+\gamma_0\gamma_1(1-\gamma_0)+\gamma_0(1-\gamma_0)(1-\gamma_1)+\gamma_0(1-\gamma_0)^2+(1-\gamma_0)^3]$$
$$\times[\frac{1}{3}((\tau+3\tau_{is})^3-(\tau+2\tau_{is})^3)-\frac{\tau}{2}((\tau+2\tau_{is})^2-(\tau+\tau_{is})^2)(2\tau+3\tau_{is})$$
$$+(3\tau\tau_{is}+\tau^2+2\tau_{is}^2)\tau_{is}]\Big\} \qquad (2.19)$$

6) System average unavailability

The average unavailability of the system is the sum of (2.12), (2.15), (2.17), and (2.19) :

$$q = q_{D'A} + q_{AB} + q_{BC} + q_{CD} \qquad (2.20)$$

When the safety system is needed at an emergency state, the probability that the safety system does not operate due to human error or due to failure of the system is as follows :

$$P_{non\_trip} = \lambda_{d\_trip}q \qquad (2.21)$$

## 2.2. Average Probability of Inadvertent Reator Trip

We derive the average probability that the reac-

tor is inadvertently tripped due to human errors or to the failure of components in a 2-out-of-3 system : G system; 't0' at the end of a sequence of renewal time (point D' in Fig.2.1). The contribution of the average probability from each interval D'A, AB, BC, CD is calculated and then added to yield the average probability.

Define the events as follows :

1) During D'A($0 \le t \le \tau$)

We have the following equations :

$$\begin{aligned}
&\Pr\{\text{reactor trip between } t \text{ and } t+dt\} \\
&= \Pr\{\text{reactor trip between } t \text{ and } t+dt | E_3E_2E_1\}\Pr\{E_3|E_2E_1\}\Pr\{E_2|E_1\}\Pr\{E_1\} \\
&+ \Pr\{\text{reactor trip between } t \text{ and } t+dt | \bar{E}_3E_2E_1\}\Pr\{\bar{E}_3|E_2E_1\}\Pr\{E_2|E_1\}\Pr\{E_1\} \\
&+ \Pr\{\text{reactor trip between } t \text{ and } t+dt | E_3\bar{E}_2E_1\}\Pr\{E_3|\bar{E}_2E_1\}\Pr\{\bar{E}_2|E_1\}\Pr\{E_1\} \\
&+ \Pr\{\text{reactor trip between } t \text{ and } t+dt | \bar{E}_3\bar{E}_2E_1\}\Pr\{\bar{E}_3|\bar{E}_2E_1\}\Pr\{\bar{E}_2|E_1\}\Pr\{E_1\} \\
&+ \Pr\{\text{reactor trip between } t \text{ and } t+dt | E_3E_2\bar{E}_1\}\Pr\{E_3|E_2\bar{E}_1\}\Pr\{E_2|\bar{E}_1\}\Pr\{\bar{E}_1\} \\
&+ \Pr\{\text{reactor trip between } t \text{ and } t+dt | \bar{E}_3E_2\bar{E}_1\}\Pr\{\bar{E}_3|E_2\bar{E}_1\}\Pr\{E_2|\bar{E}_1\}\Pr\{\bar{E}_1\} \\
&+ \Pr\{\text{reactor trip between } t \text{ and } t+dt | E_3\bar{E}_2\bar{E}_1\}\Pr\{E_3|\bar{E}_2\bar{E}_1\}\Pr\{\bar{E}_2|\bar{E}_1\}\Pr\{\bar{E}_1\} \\
&+ \Pr\{\text{reactor trip between } t \text{ and } t+dt | \bar{E}_3\bar{E}_2\bar{E}_1\}\Pr\{\bar{E}_3|\bar{E}_2\bar{E}_1\}\Pr\{\bar{E}_2|\bar{E}_1\}\Pr\{\bar{E}_1\}.
\end{aligned} \tag{2.22}$$

$$\begin{aligned}
&\Pr\{\text{reactor trip between } t \text{ and } t+dt | E_3E_2E_1\} \\
&= \Pr\{\text{reactor trip between } t \text{ and } t+dt | \bar{E}_3E_2E_1\} \\
&= \Pr\{\text{reactor trip between } t \text{ and } t+dt | E_3\bar{E}_2E_1\} \\
&= \Pr\{\text{reactor trip between } t \text{ and } t+dt | E_3E_2\bar{E}_1\} = 0 \\
&\Pr\{\text{reactor trip between } t \text{ and } t+dt | \bar{E}_3\bar{E}_2E_1\} \\
&= 2f(t)dt = 2\lambda_{ch_trip}\exp(-\lambda_{ch_trip}t)dt \\
&\Pr\{\text{reactor trip between } t \text{ and } t+dt | \bar{E}_3E_2\bar{E}_1\} \\
&= 2f(t)dt = 2\lambda_{ch_trip}\exp(-\lambda_{ch_trip}t)dt \\
&\Pr\{\text{reactor trip between } t \text{ and } t+dt | E_3\bar{E}_2\bar{E}_1\} \\
&= 2f(t)dt = 2\lambda_{ch_trip}\exp(-\lambda_{ch_trip}t)dt \\
&\Pr\{\text{reactor trip between } t \text{ and } t+dt | \bar{E}_3\bar{E}_2\bar{E}_1\} \\
&= 6f(t)F(T_{rep}) = 6\lambda^2_{ch_trip}T_{rep}\exp(-\lambda_{ch_trip}t)dt
\end{aligned}$$

Eq. (2.22) is then rewritten as

$$\begin{aligned}
P_{D'A}(t) = 2\lambda_{ch_trip}&[2(1-\gamma_0)(1-\gamma_1)\gamma_0 + \gamma_0(1-\gamma_0)^2]\exp(-\lambda_{ch_trip}t) \\
&+6\lambda^2_{ch_trip}T_{rep}(1-\gamma_0)^3\exp(-\lambda_{ch_trip}t).
\end{aligned} \tag{2.23}$$

The contribution to the average probability from D'A, i.e., the first term on the r.h.s of (2.9), is

$$\begin{aligned}
P_{av_D'A} &= \frac{\int_0^{\tau} P_{D'A}(t)dt}{\tau} \\
&= [4(1-\gamma_0)(1-\gamma_1)\gamma_0 + 2\gamma_0(1-\gamma_0)^2 + 6\lambda_{ch_trip}T_{rep}(1-\gamma_0)^3] \\
&\times[1-\exp(-\lambda_{ch_trip}\tau)].
\end{aligned} \tag{2.24}$$

2) During AB ($\tau \le t \le \tau + \tau_{ts}$)

We have the following equations :

$$\begin{aligned}
&\Pr\{\text{reactor trip between } t \text{ and } t+dt\} \\
&= \Pr\{\text{reactor trip between } t \text{ and } t+dt | E_{no_trip}E_3\bar{E}_2\bar{E}_1\}\Pr\{E_{no_trip}|E_3\bar{E}_2\bar{E}_1\} \\
&\times \Pr\{E_3|\bar{E}_2\bar{E}_1\}\Pr\{\bar{E}_2|\bar{E}_1\}\Pr\{\bar{E}_1\} \\
&+ \Pr\{\text{reactor trip between } t \text{ and } t+dt | E_{no_trip}\bar{E}_3\bar{E}_2\bar{E}_1\}\Pr\{E_{no_trip}|\bar{E}_3\bar{E}_2\bar{E}_1\} \\
&\times \Pr\{\bar{E}_3|\bar{E}_2\bar{E}_1\}\Pr\{\bar{E}_2|\bar{E}_1\}\Pr\{\bar{E}_1\}
\end{aligned}$$

$$\Pr\{\text{reactor trip between } t \text{ and } t+dt | E_{no\_trip}E_3\bar{E}_2\bar{E}_1\} = \frac{1}{\tau_{ts}}dt$$

$$\Pr\{E_{no\_trip}|E_3\bar{E}_2\bar{E}_1\} = (1-2\lambda_{ch\_trip}\tau)$$

$$\Pr\{\text{reactor trip between } t \text{ and } t+dt | E_{no\_trip}\bar{E}_3\bar{E}_2\bar{E}_1\} = 2\lambda_{ch\_trip}\tau_{ts}dt$$

$$\Pr\{E_{no\_trip}|\bar{E}_3\bar{E}_2\bar{E}_1\} = (1-6\lambda^2_{ch\_trip}T_{rep})$$

$$P_{AB}(t) = \frac{1}{\tau_{ts}}(1-2\lambda_{ch\_trip}\tau)\gamma_0(1-\gamma_0)^2 + (1-\gamma_0)^3(1-6\lambda^2_{ch\_trip}T_{rep})2\lambda_{ch\_trip} \tag{2.25}$$

The contribution to the average probability from AB, i.e., the second term on the r.h.s of (2.9), is

$$\begin{aligned}
P_{av_AB} &= \frac{\int_{\tau}^{\tau+\tau_{ts}} P_{AB}(t)dt}{\tau} \\
&= \frac{1}{\tau}\left[(1-2\lambda_{ch_trip}\tau)\gamma_0(1-\gamma_0)^2 + (1-\gamma_0)^3(1-6\lambda^2_{ch_trip}T_{rep})2\lambda_{ch_trip}\tau_{ts}\right]
\end{aligned} \tag{2.26}$$

3) During BC ($\tau + \tau_{ts} \le t \le \tau + 2\tau_{ts}$)

We have the following equations :

$$\begin{aligned}
&\Pr\{\text{reactor trip between } t \text{ and } t+dt\} \\
&= \Pr\{\text{reactor trip between } t \text{ and } t+dt | E_4\}\Pr\{E_4\} \\
&+ \Pr\{\text{reactor trip between } t \text{ and } t+dt | \bar{E}_4\}\Pr\{\bar{E}_4\}.
\end{aligned}$$

$$\Pr\{\text{reactor trip between } t \text{ and } t+dt | E_4\} = \frac{1}{\tau_{ts}}dt,$$

$$\Pr\{\text{reactor trip between } t \text{ and } t+dt | \bar{E}_4\} = 2\lambda_{ch\_trip}dt,$$

$$P_{BC}(t) = \frac{1}{\tau_{ts}}\gamma_0 + 2\lambda_{ch\_trip}(1-\gamma_0). \tag{2.27}$$

The contribution to the average probability from BC, i.e., the third term on the r.h.s of (2.9), is

$$\begin{aligned}
P_{av_BC} &= \frac{\int_{\tau+\tau_{ts}}^{\tau+2\tau_{ts}} P_{BC}(t)dt}{\tau} \\
&= \frac{1}{\tau}\left[\gamma_0 + 2\lambda_{ch_trip}\tau_{ts}(1-\gamma_0)\right]
\end{aligned} \tag{2.28}$$

4) During CD ($\tau + 2\tau_{ts} \le t \le \tau + 3\tau_{ts}$)

We have the following equations :

$$\begin{aligned}
&\Pr\{\text{reactor trip between } t \text{ and } t+dt\} \\
&= \Pr\{\text{reactor trip between } t \text{ and } t+dt | E_5\bar{E}_4\}\Pr\{E_5|\bar{E}_4\}\Pr\{\bar{E}_4\}
\end{aligned}$$

$+\Pr\{\text{reactor trip between } t \text{ and } t+dt | \bar{E}_5\bar{E}_4\}\Pr\{\bar{E}_5|\bar{E}_4\}\Pr\{\bar{E}_4\}.$

$\Pr\{\text{reactor trip between } t \text{ and } t+dt | \bar{E}_5\bar{E}_4\} = \frac{1}{\tau_{ts}}dt,$

$\Pr\{\text{reactor trip between } t \text{ and } t+dt | \bar{E}_5\bar{E}_4\} = 2\lambda_{ch\_trip}dt,$

$\Pr\{\bar{E}_5|\bar{E}_4\} = \Pr\{\bar{E}_4\} = (1-\gamma_0),$

$\Pr\{E_5|\bar{E}_4\} = \gamma_0.$

$$P_{CD}(t) = \frac{1}{\tau_{ts}}\gamma_0(1-\gamma_0) + 2\lambda_{ch\_trip}(1-\gamma_0)^2 \quad (2.29)$$

The contribution to the average probability from CB, i.e., the fourth term on the r.h.s of Eq. (2.9), is

$$P_{av\_CD} = \frac{\int_{\tau+2\tau_{ts}}^{\tau+3\tau_{ts}} P_{CD}(t)dt}{\tau}$$

$$= \frac{1}{\tau}\left[\gamma_0(1-\gamma_0) + 2\lambda_{ch\_trip}\tau_{ts}(1-\gamma_0)^2\right]. \quad (2.30)$$

6) System average probability

The average probability of the system is the sum of (2.22), (2.24), (2.26), and (2.28) :

$$P_{trip} = P_{av\_DA} + P_{av\_AB} + P_{av\_BC} + P_{av\_CD} \quad (2.31)$$

### 2.3. Optimal Inspection Period

We have two probabilities ($P_{no\_trip}$ and $P_{trip}$). We determine the weighting factors of two probabilities in order to estimate the inspection period. Then we determine the optimal inspection period that minimize the following equation :

$$y(\tau) = w_{no\_trip}P_{no\_trip}(\tau) + w_{trip}P_{trip}(\tau) \quad (2.32)$$

$w_{no\_trip}$ : weighting factor of the probability that the safety system do not operate due to human error and to failure of system.

$w_{trip}$ : weighting factor of the average probability that the reactor is tripped due to human errors or to the failure of component in a 2–out–of–3 system

The optimal inspection period is $\tau$ that satisfies the following equation :

$$\frac{dy(\tau)}{d\tau} = 0. \quad (2.33)$$

### 2.4. Comments on Human Error Probabilities

Since statistical records for the estimation of the probabilities $\gamma_0$, $\gamma_1$, ..... , $\gamma_n$ do not exist, especially for nuclear power plants, their numerical estimation is largely the result of judgment. An extensive survey of some approaches is given in Appendix III of WASH–1400[5]. Although close estimates cannot be given, it is possible to talk about the order of magnitude or the range of values of the probability of human error. The human actions of concern to us are those encountered during inspection, testing, and repair of redundant systems. Given the nature of these actions, it seems reasonable to assume that the probability of a human error committed for the first time, $\gamma_0$, is no greater than $10^{-2}$. For example, in [5], the probability of omission when there is no display in the control room of the status of the item omitted (e.g., failure to return a maintenance) is $10^{-2}$, while the probability of human error of commission (e.g., misreading a label) is $3 \times 10^{-3}$.

The conditional probabilities $\gamma_0$, $\gamma_1$, ..... , $\gamma_n$ depend on the degree of statistical dependence (coupling, as it is called in [5]) between successive human actions. The two extreme possibilities are 'no s–dependence' and 'complete s–dependence'. If there is no s-dependence, we have

$$\gamma_0 = \gamma_1 = \gamma_2 = \cdots. \quad (2.34)$$

If there is complete s–dependence, then

$$1 = \gamma_1 = \gamma_2 = \gamma_3 = \cdots. \quad (2.35)$$

In general, the degree of s–dependence will be somewhere between the two extremes, in which case we will have the bounds.

$$\gamma_0 \leq \gamma_j \leq 1, \text{ for all j.} \quad (2.36)$$

The lower bound of (2.36) can be made tighter by observing that if an error has been committed *j*

times in one period then the probability that will be committed in the next act is a non decreasing function of $j$, that is.

$$\gamma_{j-1} \leq \gamma_j \leq 1 \quad (2.37)$$

Although (2.37) is consistent with the data on human errors of [5], it should not be considered as valid in all cases.

### 3. Results

Table 4.2 and 4.3 are the new inspection periods of safety system obtained by using the method described in the previous chapter and compared with those currently used in Wolsung NPP Unit 1. Because of the lack of data for human error, we used the 95% confidence interval. We also assumed that the degree of statistical dependence between successive human actions is very low because the exact relation between successive human actions is not known generally. In other words, if there is no statistical dependence, $\gamma_0 = \gamma_1 = \gamma_2 = \cdots\cdots$. The values of the parameters used in the calculation is obtained from the data of Wolsung NPP unit 1. They are as follow : $\lambda_{ch-trip} = 3.4 \times 10^{-4}$, $\lambda_{d-trip} = 1.8 \times 10^{-5}$, $\gamma_0 = \gamma_1 = \gamma_2 = 8.24 \times 10^{-6} \sim 4.44 \times 10^{-4}$ (confidence interval of 95%), $\tau_{ts} = 15$minutes, $w_{no-trip} = 0.999$, $w_{trip} = 0.001$.

The failure rates of safety system for trip parameters are listed in Table 4.1.

As a consequence, the inspection periods obtained using a minimum human error ($8.24 \times 10^{-6}$) are shorter than those used in Wolsung

**Table 4.1. Failure Rates of Shutdown System for Trip Parameters**

| Trip Parameter | Failure Rates of SDS 1 (1/hour) | Failure Rate of SDS 2 ($10^{-7}$) |
|---|---|---|
| Neutron Overpower | $1.36 \times 10^{-4}$ | $1.12 \times 10^{-4}$ |
| High Rate Log N Power | $1.36 \times 10^{-4}$ | $1.11 \times 10^{-4}$ |
| Pressurizer Low Level | $3.51 \times 10^{-5}$ | $2.75 \times 10^{-5}$ |
| Boiler Low Level | $3.51 \times 10^{-5}$ | $2.75 \times 10^{-5}$ |
| HTS Low Flow ( SDS 1 ) | $3.29 \times 10^{-5}$ | $2.53 \times 10^{-5}$ |
| HTS Low Differential Pressure (SDS 2) | | |
| Boiler Feed line low Pressure | $3.26 \times 10^{-5}$ | $2.56 \times 10^{-5}$ |
| HTS Low Pressure | $3.44 \times 10^{-5}$ | $2.66 \times 10^{-5}$ |
| HTS High Pressure | $3.26 \times 10^{-5}$ | $2.49 \times 10^{-5}$ |

**Table 4.2. Comparison of the Inspection Periods of SDS 1 Obtained by the Method Proposed in this Paper and Those Used in Wolsung NPP Unit 1**

| Trip Parameter | Inspection Periods used in Wolsung | Inspection Periods obtained using the new method with a confidence interval of 95 % |
|---|---|---|
| Neutron Overpower | 1 week | 5 ~ 16 days |
| High Rate Log N Power | 1 week | 5 ~ 16 days |
| Pressurizer Low Level | 1 month | 20 ~ 42 days |
| Boiler Low Level | 1 month | 20 ~ 42 days |
| HTS Low Flow | 1 month | 20 ~ 43 days |
| Boiler Feed line low Pressure | 1 month | 20 ~ 44 days |
| HTS Low Pressure | 1 month | 20 ~ 42 days |
| HTS High Pressure | 1 month | 20 ~ 44 days |

**Table 4.3. Comparison of the Inspection Periods of SDS 2 Obtained by the Method Proposed in this Paper and Those Used in Wolsung NPP Unit 1**

| Trip Parameter | Inspection Periods used in Wolsung | Inspection Periods obtained using the new method with a confidence interval of 95 % |
|---|---|---|
| Neutron Overpower | 1 week | 5 ~ 19 days |
| High Rate Log N Power | 1 week | 5 ~ 19 days |
| Pressurizer low Level | 1 month | 23 ~ 49 days |
| Boiler Low Level | 1 month | 23 ~ 49 days |
| HTS Low Differential Pressure | 1 month | 24 ~ 52 days |
| Boiler Feed line Low Pressure | 1 month | 24 ~ 51 days |
| HTS Low Pressure | 1 month | 23 ~ 50 days |
| HTS High Pressure | 1 month | 23 ~ 52 days |

NPP unit 1 whereas the inspection periods obtained using a maximum human error ($4.44 \times 10^{-4}$) is longer than those used in Wolsung NPP unit 1.

## 4. Conclusions and Further Study

The engineered safeguards of Wolsung NPP unit 1 contain redundant system of 2–out–of–3 logic which are not operating under normal conditions but are called upon to act when emergency conditions develop. In this paper, taking into account the failure probability of channel due to human error in the simultaneous testing scheme, unavailability formulae for 2–out–of–3 logic configurations are developed. The failure probability of the channel due to human error is assumed to be independent of the number of channels which have gone through the tests consecutively prior to the inspection of the channel under consideration. The result shows that the inspection periods obtained using a minimum human error ($8.24 \times 10^{-6}$) are shorter than those used in Wolsung NPP unit 1 whereas the inspection periods obtained using a maximum human error ($4.44 \times 10^{-4}$) is longer than those used in Wolsung NPP unit 1. Because of the lack of data for human error, the range of 95 % confidence interval is wide. Therefore the optimal inspection period obtained using the method of this work have the value of wide range.

The development in this work is on the conservative side since no credit has been given to possible feedback which might alert the operator to the fact that successive errors are being committed (recovery–factor as discussed in [2]). If such a feedback were included in the analysis, our assumption that the human error probabilities are s–independent of the period would be invalid and Eq. (2.29) would not be true even within the same period. The development of mathematical models considering the feedback and the derivation of the corresponding unavailability formulae would be considerably involved.

### Nomenclature

| | |
|---|---|
| E1 | operator errs in A'B' |
| E2 | operator errs in B'C' |
| E3 | operator errs in C'D' |
| E4 | operator errs in AB |
| E5 | operator errs in BC |
| $E_{no-trip}$ | no trip |
| f(t) | failure probability density function |
| F(t) | cumulative distribution function |
| i. f. f | if only and if |

| | |
|---|---|
| i. i. d | identically independent distribution |
| $p_f$ | probability that system is failed during the testing time, taking into account the probability of failure of components due to human error or of failure of hardware |
| Pr {t} | probability function of time |
| q | average unavailability |
| Q(t) | unavailability |
| s–independence | statistical independence |
| $T_{rep}$ | repairing time |
| $w_{no-trip}$ | weighting factor for the probability that the safety system do not operate due to human error or due to failure of components |
| $w_{trip}$ | weighting factor for the average probability that the reactor is tripped due to human error or due to failure of components in a 2–out–of–3 logic configuration |

**Greek Letters**

| | |
|---|---|
| $\gamma_0$ | probability the operator errs for the first time in one period |
| $\gamma_j$ | j = 1, ....., (n–1); conditional probability of the human error being repeated for the (j+1) times given that it has occurred for j consecutive times in the current period |
| $\lambda_{d-trip}$ | occurrence rate of trip |
| $\lambda_{ch-trip}$ | occurrence rate of channel trip |
| $\tau$ | inspection interval |
| $\tau_t^s$ | testing time |

## References


1. 한국 전력공사 기술연구원, "The Reliability Analysis of Special Safety Systems for the Availability Improvement of Wolsung NPP Unit", KRC – 87N – JO3, 1989.
2. G. E. Apostolakis, and P.P. Bansal, " Effect of Human Error on the Availability of Periodically Inspected Redundant Systems," IEEE Transaction. on Reliability Vol. R–26, No.3, August, 1977.
3. G. E. Apostolakis, and T.L. Chu, "The Unavailability of Systems under Periodic Test and Maintenance," Nuclear Technology, Vol. 50, August, 1980
4. George. J. Anders, "Human Failure Considerations in Determining an Optimal Inspection Interval for Equipment Used in Emergency Conditions", IEEE Transaction on Systems, Man, and Cybernetics, Vol. SMC–15, No. 2, March/April 1985.
5. Reactor Safety Study, "An Assessment of Accident Risks in U. S. Commercial Nuclear Power Plants WASH – 1400, USNRC, Oct. 1975.
6. A. E. Green, A. J. Bourne, "Reliability Technology", Wiley–Inter–science, London, 1972.
7. R. E. Barlow, F. Proschon, "Statistical Theory of Reliability and Life Testing", Holt, Rinehart and Winston, New York, 1975.