Journal of the Korean Nuclear Society
Volume 15, Number 4, December, 1983

《**Original**》

The Common Mode Failures Analysis of The Redundant System with Dependent Human Error

Myung Ki Kim and Soon Heung Chang

Korea Advanced Institute of Science and Technology

(Received September 5, 1983)

의존적 인간 실수를 고려한 중복 시스템의 Common Mode Failures의 분석

김 명 기·장 순 흥

한국과학기술원

(1983. 9. 5 접수)

Abstract

Common Mode Failures (CMFs) have been a serious concern in the nuclear power plant. There is a broad category of the failure mechanisms that can cause common mode failures. This paper is a theoretical investigation of the CMFs on the unavailability of the redundant system. It is assumed that the total CMFs consist of the potential CMFs and the dependent human error CMFs. As the human error dependence is higher, the total CMFs are more effected by the dependent human error. If the human error dependence is lower, the system unavailability strongly depends on the potential CMFs, rather than the mechanical failure or the dependent human error. And it is shown that the total CMFs are dominant factor to the unavailability of the redundant system.

요 약

원자력발전소에서 Common Mode Failures (CMFs)가 상당한 관심을 모으고 있다. 이 논문에서는 중복 시스템의 비가용도(Unavailability)에 있어서의 전체 CMFs를 잠재적 CMFs(Potential CMFs)와 의존성 인간 실수에 의한 CMFs (CMFs of dependent human error)로 나누어 이론적으로 고찰하였다. 결론적으로, 인간 실수의 의존성이 높아질수록 전체 CMFs는 의존성 인간실수에 의해서 주로 영향을 받는다고 할 수 있다. 역으로, 인간 실수의 의존성이 낮아질수록, 전체 시스템의 비가용도는 기계적 고장이나 의존성 인간실수보다 잠재적 CMFs에 의해 지배된다고 할 수 있다. 그리고, 중복 시스템의 비가용도에 있어서 전체 CMFs가 기계적 고장보다 주된 요소임도 알 수 있었다.

1. Introduction

There are engineered safety systems in the nuclear power plant. These systems require high reliability, therefore they should have a redundant system. But the benefit of redundant system is limited by the possibility of simultaneous

failure of all redundant systems due to a common mode failures(CMFs) or common cause failure (CCFs).

The analysis of common mode failures may be difficult because of the various considerations to be made, such as the recognition of many possible causes of common mode failures and the means of identification, etc..

The recommended methods against common mode failures are naturally based on different forms of the diversity. By using different types of equipment, more than one logical way to monitor the state of the system, physically separating redundant components, having more than one operator to review personal actions, and employing other forms of the diversity, it is resonable to expect that the probability of common mode failures is reduced.

This work is a theoretical investigation of the importance of common mode failures on the unavailability of redundant systems, and it is assumed that the CMFs are divided into the common mode failures resulting from the human error during the maintenance, and the potential common mode failures caused by other factors, such as earthquakes, explosions, and fires, etc.. And the human error during the maintenance is considered as a dependent human error.

In the U.S. nuclear power plants, for 228 reactor-years of experience, there are 7038 citations, among which 1490 or 21% were identified as cuased by the human error [1]. This human error rate is about the same as in other industries. From above experiences during the maintenance, the human error per task was estimated to be 1.4×10^{-3}. This rate is dominant over the other human errors which are generally reted at $10^{-5}\sim10^{-4}$. This results from the fact that the system is not well designed for the inspector who tests the whole system periodically. As an example, some of the components are installed beyond reach and too high in evaluation to test. Here, the potential common mode failures would affect the group of components so that all the components can be simultaneously destroyed by the potential common mode failures which occurs at a rate λ_{cm}, which has to be estimated using a variable data, if any, or mainly engineering judement. The total common mode failures is given as follows:

$$(CMFs)_t=(CMFs)_h+(CMFs)_p$$

This paper presents an estimation on the unavailability of the system with two kinds of common mode failures, that is, the common mode failures resulting from the human error during the maintenance and the common mode failures resulting from other facts with exception of the human error during the maintenance.

The estimation of common mode failures on the reliability of redundant systems has been discussed in the reference [2] and a borad category of failure mechanisms that can cause common mode failures in redundant systems and other high-reliability systems are as follows [3]:

(1) Design deficiency: failures from unrecognized component or system dependence on a signle, common element or service.

(2) Functional deficiency: a misapplication of hardware of an inability to predict the true nature of the plant variable.

(3) External environment: failures from contamination of fluid system, corrosion, and electircal noise, etc..

(4) External phenomena: failures from natural disasters, such as earthquake, fire, flood, storm, and termperature extremes.

(5) Human factor: failures from clumsiness, absent mindedness, deliberate misoperation, and inadvertent responses.

The common antidote for CMF seems to be the diversity. Accordingly, the reference [4-7] classified five kinds of diversity.

(1) Functional diversity: the use of different

plant parameters to provide protection of an event.

(2) Operational administrative diversity: different persons to do certain tasks or a second person to check on the first.

(3) Design administrative diversity: design reviews, qualification testing.

(4) Equipment diversity: providing different equipments to measure the same parameter.

(5) physical diversity: physical separation of instrumentations and components measuring the various key parameters.

2. Notations and Assumptions

The notations and assumptions in this study are as follows:

(1) The components of the system are sequentially inspected.

(2) The component is down during the test time and it is sufficiently to restore the component to the good state during the maintenance time.

(3) If the human error takes place during the maintenance, the component is completely to be out of order.

(4) The total CMFs consist of the potential CMF and the human error CMF.

(5) The potential CMF is random variable and is rated at λ_{cm}

(6) The dependent human errors are expressed as follows:

r_0: probability that the operator errs for the first time in one period.

r_j: conditional probability of the human error being repeated for the $(j+1)$ time given that it has occured for j consecutive times in the current period.

(7) In the Boolean domain, Boolean variables by which the path-set is expressed are denoted by lower alphabetic symbol, $(a,b,\cdots)$, and in the probability domain, probabilistic variables are denoted by $R_a(t)$, $R_b(t)$,$\cdots$ in the given time interval.

(8) The average unavailability during the test interval T is defined as

$$q=\frac{1}{T}\int_0^T F(t)\,dt$$

$F(t)$ is expressed by the product of the probability of the human error event by the probability of the system failure in the given time interval T.

(9) The human error events are defined as follows:

e_i: the event that operator tests the component i

if $e_i=1$: the operator does not err during the maintenance of the component i

if $e_i=0$: the operator errs during the test time of the component i.

(10) It is assumed that the human error has five level dependences [8]

1. Zero dependence: $r_N=r_0$
2. Low dependence: $r_N=(1+19r_0)/20$
3. Moderate dependence: $r_N=(1+6r_0)/7$
4. High dependence: $r_N=(1+r_0)/2$
5. Complete dependence: $r_N=1$

where, r_N is the error rate for the Nth action.

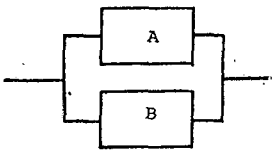
3. 1-Out-Of 2 System: Unavailability

The modelling of a system with dependent human error and potential CMF is depicted in Fig-1, and the inspector tests sequentially A and B. Here, the maintenance time is usually a few hours (bt the test period is one month), so that the maintenance time is neglected for the simple calculation.

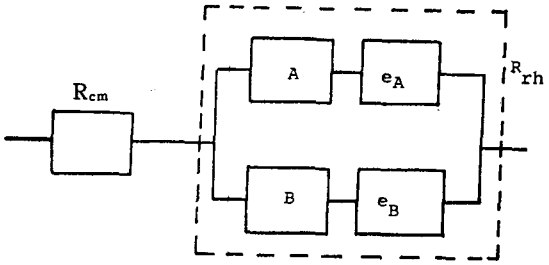
Firstly, the unavailability of the system with exception of the potential CMF is calculated, and the minimal path-set is as follows except R_{cm}

$$P=a\cdot e_A+b\cdot e_B \cdots\cdots (1)$$

The modified Karnaugh Map of the system



(a) The Block-diagram of the 1-out-of-2 System



rh=random and human error
cm=common mode failure

(b) The Block-diagram of the 1-out-of-2 System with CMFs.

Fig. 1. The Modeling of the 1-out-of-2 System

$e_A e_B$ \ ab	00	01	11	10	Human Error Rate
00	0	0	0	0	$r_0 r_1$
01	0	1	1	0	$r_0(1-r_1)$
11	0	1	1	1	$(1-r_0)^2$
10	0	0	1	1	$(1-r_0)r_0$

Fig. 2. The Modified Karnaugh Map of the 1-out-of-2 System with Human Error

without the potential CMF divided from the equation (1) is depicted in Fig-2. From Fig-2, each group is estimated as follows

$$F_{rh}=r_0r_1 \quad \text{for 1st row}$$
$$+r_0(1-r_1)\bar{R}_B \quad \text{for 2nd row}$$
$$+(1-r_0)r_0\bar{R}_A \quad \text{for 3rd row}$$
$$+(1-r_0)^2\bar{R}_A\bar{R}_B \quad \text{for 4th row}$$
$$\cdots\cdots\cdots\cdots(2)$$

$F_{rh}=1-R_{rh}$, $\bar{R}_A=1-R_A$

(1) If the mechanical components are in perfectly good states, then $\bar{R}_A=\bar{R}_B=0$, the system is failed by only human error. CMF probability resulting from human error is

$F_1=r_0r_1$

(2) If the inspector perfectly tests the component, so, there is no human error during the maintenance, the system is subjected to the mechanical component failure: $r_0=r_1=0$

$F_2=\bar{R}_A\cdot\bar{R}_B$

(3) The system failure that results from the human error and the mechanical failure is as follows

$$F_3=r_0(1-r_1)\bar{R}_B+(1-r_0)r_0\bar{R}_A$$
$$-r_0(2-r_0)\bar{R}_A\bar{R}_B$$

that is,

$F_{rh}=F_1+F_2+F_3$

The total failure of the 1-out-of-2 system considering the potential CMF is as follows

$F_{cm}=1-\exp(-\lambda_{cm}\cdot t)$

$$F_t=F_{rh}+F_{cm}-F_{rh}F_{cm}$$
$$=F_1+F_2+F_3+F_{cm}-(F_1+F_2+F_3)F_{cm}$$
$$=F_1+F_2+F_3+(1-F_1-F_2-F_3)F_{cm} \quad \cdots(3)$$

Here, the value of the system failure resulting from the human error CMF and the potential CMF is given as: $F_2=F_3=0$.

$F_{t1}=F_1+(1-F_1)F_{cm}$

so, the unavailability of system is the averaged-value of F_{t1}

$$q_{t1}=\frac{1}{T}\int_0^T F_{t1}dt$$
$$=\frac{1}{T}\int_0^T\{r_0r_1+[1-\exp(-\lambda_{cm}\cdot t)]$$
$$-r_0r_1[1-\exp(-\lambda_{cm}\cdot t)]\}dt$$
$$=1-\frac{(1-r_0r_1)}{T\cdot\lambda_{cm}}[1-\exp(-\lambda_{cm}\cdot T)]$$

If the inspector perfectly tests the components, then there is no human error in the maintenance, the system failure results from the potential CMF and the mechanical component failure.

$F_{t2}=F_2+(1-F_2)F_{cm}$

$$q_{t2}=\frac{1}{T}\int_0^T F_{t2}dt$$
$$=\frac{1}{T}\int_0^T[\bar{R}_A\bar{R}_B+(1-\bar{R}_A\bar{R}_B)(1-\exp$$
$$(-\lambda_{cm}\cdot t))]dt$$

The human error and the mechanical failure and the potential CMF concurrently effect the system failure.

Table 1. The Unavailability of the 1-out-of-2 System

Dependence	Rate	q	q_{t1}	$r_0 r_1$	*percentage (%)
Z D	$r_N=r_0$	4.36×10^{-4}	4.11×10^{-4}	10^{-6}	94
L D	$r_N=\frac{1+19r_0}{20}$	4.86×10^{-4}	4.62×10^{-4}	5.1×10^{-5}	95
MD	$r_N=\frac{1+6r_0}{7}$	5.78×10^{-4}	5.55×10^{-4}	1.44×10^{-4}	96
H D	$r=\frac{1+r_0}{2}$	9.34×10^{-4}	9.11×10^{-4}	5×10^{-4}	97.5
C D	$r_N=1$	1.43×10^{-3}	1.41×10^{-3}	10^{-3}	98.6

*$q_{t1}\div q\times100(\%)$

$$F_{t3}=F_3-(1+F_3)F_{cm}$$

$$q_{t3}=\frac{1}{T}\int_0^T[F_3-(1+F_3)F_{cm}]dt$$

The total unavailability of the 1-out-of-2 system with including the potential CMF and the dependent human error is as follows.

$$q=q_{t1}+q_{t2}+q_{t3}$$

For example, set $\lambda_{cm}=10^{-2}[yr^{-1}]$, $\lambda_A=\lambda_B=10^{-5}[hr^{-1}]$ and $r_0=10^{-3}$.

The results is described in Table-1.

4. Example

Consider, as an example, the Simplified Auxiliary Feed Water System (AFWS) of a nuclear power plant (Fig-3), consisting of two tanks in parallel, T_1 and T_2, in series with a parallel system of pumps (P_1,P_2,P_3) and valves (V_1, V_2, V_3). The inspecter tests the values periodically. So, the human erros take place during the maint enance and these erros are mutually dependent because the inspector tests component by the same procedures and the same methods. And the potential common mode failure resulting from fires, explosions, earthquakes, and the contamination in oil, etc., must be considered, because these causes the system to fail simultaneously. It is assumed that each pump supply the water sufficiently to the steam generator, and the periodic test is accomplished in a given time (a few hours), however this time period is less than the test interval and the test time is neglected for the simple calculation. The Block-diagram of the system with the dependent human error and the potential CMF is depicted in Fig. 4.

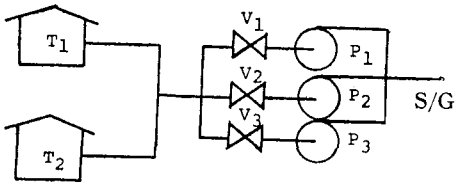


Fig. 3. The Simplified Diagram of the Auxiliary Feedwater System of a Nuclear Power Plant

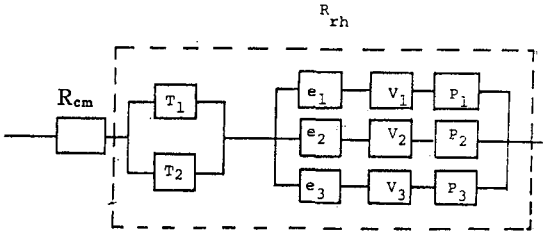


Fig. 4. The Block-diagram of the AFWS with CMFs

For R_{hr}, from the Fig. 4, the minimal path-set is as follows

$$P=e_1V_1P_1+e_2V_2P_2+e_3V_3P_3$$

From the minimal path-set, the modified Karnaugh Map is derived in Fig-5. From the modified Karnaugh Map, the each row that describes the system failure is as follows.

$$\begin{aligned}F_{vp}=&r_0r_1r_2+r_0r_1(1-r_2)\bar{C}+r_0(1-r_1)\bar{B}\bar{C}\\&+r_0(1-r_1)r_1\bar{B}+(1-r_0)^2r_0\bar{A}\bar{B}\\&+(1-r_0)^3\bar{A}\bar{B}\bar{C}+(1-r_0)r_0(1-r_1)\bar{A}\bar{C}\\&+(1-r_0)r_0r_1\bar{A}\end{aligned}$$

where, $A=R_{v1}R_{p1}$, $B=R_{v2}R_{p2}$, $C=R_{v3}R_{p3}$

$e_Ae_Be_C$ \ abc	000	001	011	010	110	111	101	100	Human Error Rate
000	0	0	0	0	0	0	0	0	$r_0r_1r_2$
001	0	1	1	0	0	1	1	0	$r_0r_1(1-r_2)$
011	0	1	1	1	1	1	1	0	$r_0(1-r_1)^2$
010	0	0	1	1	1	1	0	0	$r_0r_1(1-r_1)$
110	0	0	1	1	1	1	1	1	$(1-r_0)^2r_0$
111	0	1	1	1	1	1	1	1	$(1-r_0)^3$
101	0	1	1	0	1	1	1	1	$(1-r_0)r_0(1-r_1)$
100	0	0	0	0	1	1	1	1	$r_0r_1(1-r_0)$

Fig. 5. The Modified Karnaugh Map of the AFWS with the Dependent Human Error

vp=valve and pump

The total unavailability of the system is as follows.

$$F=F_{cm}+F_T+F_{vp}-F_{cm}F_T-F_TF_{vp}-F_{vp}F_{cm}+F_{cm}F_TF_{vp}$$

where

$$F_T=\bar{R}_{T1}\bar{R}_{T2}$$

$$F_{cm}=1-\exp(-\lambda_{cm}\cdot t)$$

The total CMFs which consist of the human error and the potential CMF is defined as follows:

$$q_{cm}=\frac{1}{T}\int_0^T\{r_0r_1r_2+[1-\exp(-\lambda_{cm}\cdot t)]-r_0r_1r_2[1-\exp(-\lambda_{cm}\cdot t)\}\,dt$$

$$=1-\frac{1-r_0r_1r_2}{T\cdot\lambda_{cm}}(1-\exp(-\lambda_{cm}\cdot T)$$

As an example, set each component failure rate $\lambda=10^{-5}[\mathrm{hr}^{-1}]$ and the potential channels of nuclear reactor have a typical CMF rate: $\lambda_{cm}=10^{-2}[\mathrm{yr}^{-1}]$, $10^{-3}[\mathrm{yr}^{-1}]$; $[10^{-2}(\mathrm{yr}^{-1})=1.14\times10^{-6}[\mathrm{hr}^{-1}]$, $10^{-3}(\mathrm{yr}^{-1})=1.14\times10^{-7}[\mathrm{hr}^{-1}]]$, so it is assumed the CMFs rate of the AFWS is $10^{-2}[\mathrm{yr}^{-1}]$, $10^{-3}[\mathrm{yr}^{-1}]$, and the system is tested every one month [720hrs] and the first human error rate r_0 is 10^{-3}.

The results are described in Table 2.

From Table 2, we concluded that the quantitative of the total CMFs result from the potential CMFs in case of low human error dependence and the quantitative of the total CMFs result from the human error in case of high human error dependence.

And the total unavailability of the system is effected by the total CMFs, rather than the system hardware failure, in any case, $\lambda=10^{-2}$

Table 2. The Unavailability of the AFWS Considering the Human Error and the Potential Common Mode Failure

Dependence	$\lambda_{cm}=10^{-2}(\mathrm{yr}^{-1})[1.14\times10^{-6}\mathrm{hr}^{-1}]$			$\lambda_{cm}=10^{-3}(\mathrm{yr}^{-1})[1.14\times10^{-7}\mathrm{hr}^{-1}]$			$r_0r_1r_2$
	Total Unavailability	Total CMF	*Percentage	Total Unavailability	Total CMF	*Percentage	
Z D	4.229×10^{-4}	4.1×10^{-4}	97%	5.39×10^{-5}	4.1×10^{-5}	76%	10^{-9}
L D	4.255×10^{-4}	4.12×10^{-4}	97%	5.65×10^{-5}	4.37×10^{-5}	77%	2.6×10^{-6}
M D	4.44×10^{-4}	4.3×10^{-4}	97%	7.46×10^{-5}	6.166×10^{-5}	82%	2.06×10^{-5}
H D	6.73×10^{-4}	6.6×10^{-4}	98%	3.044×10^{-4}	2.9×10^{-4}	95%	2.5×10^{-4}
C D	1.423×10^{-3}	1.41×10^{-3}	99%	1.054×10^{-3}	1.04×10^{-3}	98%	10^{-3}

$F_{cm}=4.1\times10^{-4}[\lambda_{cm}=10^{-2}\mathrm{yr}^{-1}]$

$=4.1\times10^{-5}[\lambda_{cm}=10^{-3}\mathrm{yr}^{-1}]$

*Total CMFs÷Total unavailability×100

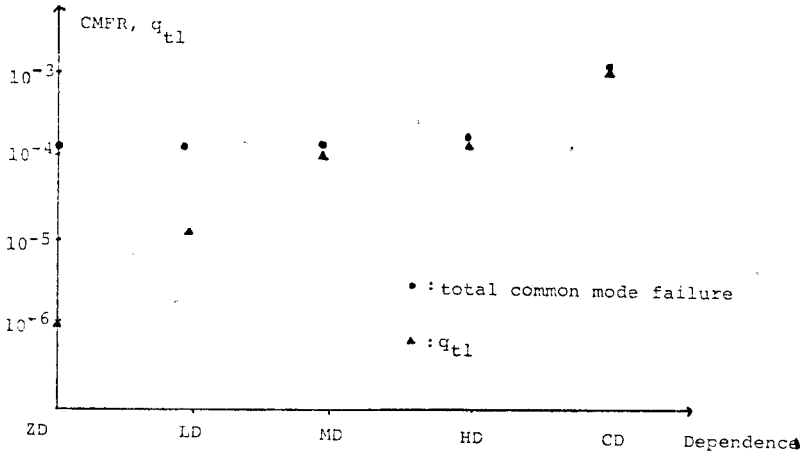


Fig. 6. The CMFR vs. Dependence

$[yr^{-1}]$, $\lambda=10^{-3}[yr^{-1}]$.

5. Results

This paper is a theoretical investigation of the dependent human error and the potential common mode failure on the unavailability of redundant systems.

There are many kinds of CMFs, but in this paper, the CMFs are divided into the common mode failure resulting from the human error and the potential common mode failure. The potential common mode failure is assumed to be the result of fatal shocks, e.g., earthquakes, fires, and explosions, which occur at a constant rate, λ_{cm}. This rate has to be estimated using available data, if any, and mainly engineering judgement. Apostolakis[2] assumed that the protection channel of nuclear reactors have a typical CMFs rate $\lambda_{cm}=10^{-2}[yr^{-1}]$, so this upper considered the potential CMFs rate, λ_{cm}, as the paper value.

From Table 1, the unavailability of the system is mainly infludenced by the common mode failures, q_{t1}, that is, the key failure element is the common mode failures. As the human error dependence becomes complete dependence, the human error CMFs is dominant over that of other kinds of dependences.

References

1. I.A. Watson, "Common Mode Failures in Redundancy Systems", *Nuclear Technology*, 46, p. 183-191, (Dec. 1979).
2. G.E. Apostolakis, "Effect of a Certain Class of Potential Common Mode Failures on the Reliability of Redundant Systems", *Nucl. Eng. Des.*, 36, p. 220-231, (1976).
3. I.M. Jacobs, "The Common Mode Failure Study Discipline", *IEEE Trans. Nuclear Sci.*, NS. 17, 1, p. 594-598 (Feb. 1970).
4. G.E. Apostolakis, "Effect of Human Error on the Availability of Periodically Inspected Redundant Systems", *IEEE Trans. Reliability*, R-26, 3, p. 220-225 (Aug. 1977).
5. M.E. Jolly and J. Wreathall, "Common-Mode Failures in Reactor Safety Systems", *Nucl. Safety*, 18, 5 (1977).
6. E.W. Hagen, "Common-Mode/Common Cause Failure: A Review", *Nucl. Safety*, 21, No. 2, (1980).
7. K.C. Hayden, "Common-Mode Failure Mechanisms in Redundant Systems Important to Reactor Safety", *Nuclear Safey*, 17, No. 6, p. 686-693, (1976).
8. G.E. Apostolakis, "Data Analysis in Risk Assessments," *Nuclear Engineering and Design*, 71, p. 375-381, (1982).
9. "Reactor Safety", WASH-1400(NUREG-75/014). USNRC, Oct. (1975).