Journal of the Korean Nuclear Society
Volume 11, Number 3, September, 1979

《**Original**》

Evaluation of Unavailability of the Containment Spray System by Use of a Cause-Consequence Chart

Gwi Tae Park, Hee Young Chun

Korea University

Chang Kun Lee

Korea Atomic Energy Research Institute

(June 12, 1979)

Abstract

In this paper, a cause-consequence chart is applied to evaluate the probability that the containment spray system in a nuclear power plant may not be woring properly, given a demand for spryaing at loss of coolant accident (LOCA). It is shown how the diagram provides a basis for calculating two probability measures for malfunctioning of this system, in case the test policy of the system is taken into account, i.e., average probability that the containment spray cannot be established, and average probability that the containmennt spray is established; spray stops before the required operating time is over.

1. Introduction

In the design of unclear power plants, accident analysis may be motivated in order to protect important facilities or to reduce those consequences of failure that may lead to the enviornmental contamination or risk to human life. The purpose of accident analysis is to provide a basis for assessment of the probability of all accidents and evaluation of their consequences (risk analysis). Risk analysis requires a systematic follow-through of the different accident courses that a specified abnormal event can lead to. This can be done by means of various methods such as fault tree & event tree, fault tree, cause-consequence chart, etc.[1~4] Among them, the cause-consequence chart gives a simpler representation of event sequences and the conditions under which these events can take place.

The purpose of this paper is to demonstrate the application of a cause-consequence chart to a specific system. The containment spray system in a pressurized-water reactor is analyzed in this research. Loss of coolant accident may be caused by a break in the primary loop boundary. To reduce the pressure and iodine concentration in the containment at LOCA, the plant is equipped with the containment spray system consisting of two redundant spray subsystems with 100% capacity each. If a demand for

operation of the containment spray system arises, both subsystems are inserted.

2. System Description[5]

Fig. 1 is a simplified flow diagram of the containment spray system. The valve positions shown in Fig. 1 are for normal plant operation. In order to operate both subsystems A and B simultaneously, valves V_{3A} or V_{4A} and V_{3B} or V_{4B} must be opened and pumps P_A and P_B must be started. In the event of a large LCCA, this would normally be done by a signal from the sequence limiting control system. In each system a motor pump P_A or P_B takes suction from the refuelling water storage tank (RWST). Each subsystem is separately taken out of standby status for monthly flow test of pumps. For this test, the manual valve V_{6A} or V_{6B} is opened to allow a return path to the RWST for the pump flow.

Each of the two subsystems A and B is applied from separate bus system connected to the power lines. For each bus system an emergency diesel generator backs up to power supply.

System A can be considered as consisting of two subsystems A_1 and A_2, connected in series. During normal reactor operation the components in A_1 and B_1 are tested at regular intervals of time τ_1 and repaired or replaced if faulty. In Fig.1 this corresponds to the components that can be tested by leading water back to RWST plus the containment isolation valves V_{3A} and V_{4A}. Subsystems A_2 and B_2 consist of the remaining components in A and B, respectively. A thorough proof testing of the total system takes place at interval $\tau_2=m\tau_1$ (m is an integer) during scheduled reactor shutdown.

In case of LOCA, the reactor is shutdown. The containment spray system is then required to operate for a certain time t_0. If only one system is activated on demand for spraying, repair of the other system will be carried out if the failed components are accessible, i.e., if they belong to either subsystem A_1 or B_1. After repair the system is inserted. If one of the redundant spray systems fails during the required operation period t_0, then repair is started if possible. After repair the system is restarted.

A fault can be characterized as either "announced" or "unannounced". An announced fault "reveals itself" and normally leads to immediate maintenance action. Unannounced faults are disclosed by testing, and the

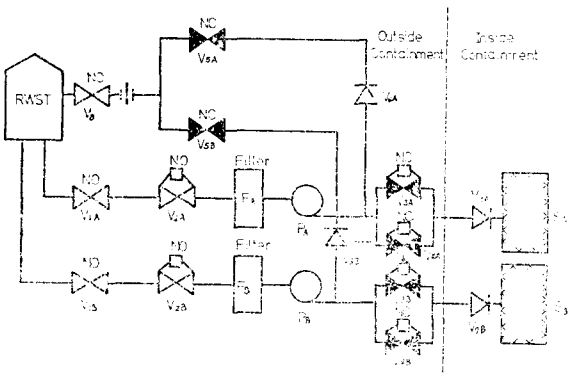

Fig.1. Simplified flow diagram of containment spray system

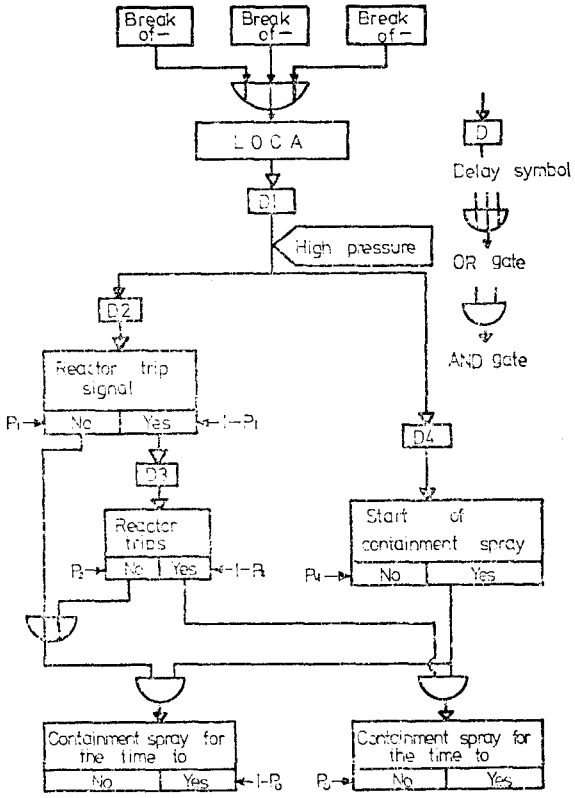

Fig.2. Consequnce chart for "loss of coolant."

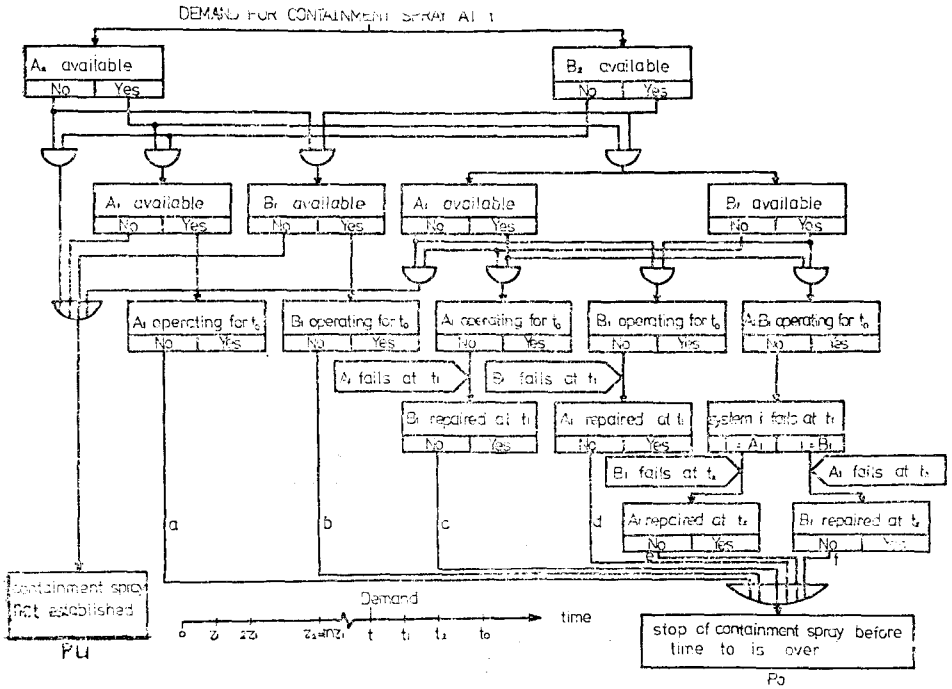

Fig.3. Consequence chart for containment spray system

failed components are repaired or replaced.

3. Cause-consequence Analysis

Fig.2 is a partly developed consequence chart that defines and presents the most probable accidents. The diagram focuses on two failure modes of the containment spray system:

1) The system is unavailable when called upon.
2) The system fails before the required operating time t_0 is over.

As a basis for evaluating a suitable unreliability measure for the system, a failure analysis is performed by developing a cause-consequence chart for the system to the necessary level. The diagram consists of the consequence chart in Fig.3 with the following associated cause charts:

1) Subsystem A_1 is unavailable (Fig.4)
2) Subsystem A_2 is unavailable (Fig.4)
3) Subsytsem B_1 is unavailable (similar to diagram 1)
4) Subsytem B_2 is unavailable (similar to diagram 2)
5) Failure of subsystem A_1 (Fig.5)
6) Failure of subsystem B_1 (similar to diagram 5)

Cause charts 5 and 6 are valid for the operating time following a random demand. The input events for an individual diagram are assumed to be statistically independent.

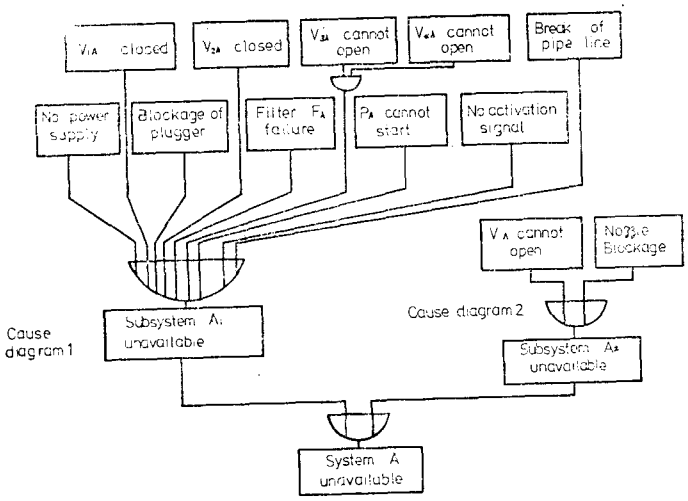

Fig.4. Cause chart for system A is unavailable

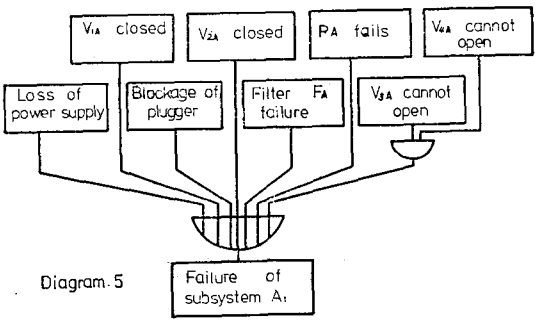

Fig.5. Cause chart for "Failure of subsystem A1"

4. Probability Evaluation

4.1. Problem Formulation

Our aim is to evaluate system unreliability measures to be used in connection with risk analysis, test policy planning, etc. We shall outline the evaluation of the following probabilities.

$P_u \equiv$ Average Pr (Containment spray connot be established | a demand for sprying)

$P_0 \equiv$ Average Pr (Containment spray is establised; spray stops before the required operating time t_0 is over | a demand for spraying)

The average is here taken over the problem time T, the "lifetime" of the plant.

4.2. Notations

t_0: required operating time of containment spray system during an emergency.

τ_1: test interval for components in subsystem A_1 and B_1.

τ_2: thorough proof testing interval for all components in system A and B; $\tau_2 = m\tau_1$, where m is an integer.

T: problem time, ("lifetime" of the plant) $T = n\tau_1 = \frac{n}{m}\tau_2$, where $\frac{n}{m}$ is an integer.

i: subscript referring to either system A or B or the subsystems of these A_1, A_2, B_1, B_2.

$P_i(t)$: Pr {system (subsytem) i cannot be activated at time t}

$(P_i)_{av}$: average valve of $P_i(t)$ within the problem time T.

P_u: average Pr (containment spray cannot be established | demand for spraying)

$F_i(t)$: Cdf of time to on-line failure of subsystem A_1 or B_1.

$f_i(t)$: pdf corresponding to $F_i(t)$.

$G_j(t)$: Pr (event sequence j occurs | demand for spraying at time t) ($j=a$ to f in Fig.3)

$(G_j)_{av}$: average valve of $G_j(t)$ within the problem time T.

P_0: average Pr (containment spray is established; spray stops before t_0 is over | demand for spraying)

P_s: average Pr (system failure | demand for spraying)

$Q_i(t)$: Cdf of time to repair of unannounced failure of subsystem A_1 or B_1.

$R_i(t)$: Cdf of time to repair of on-line failure of subsystem A_1 or B_1.

—: implies the ones complement, e.g., $\bar{\mathfrak{Q}} \equiv 1 - \mathfrak{Q}$

4.3. Assumptions

(1) All component faults causing a system to be unavailable when called upon are considered to be unannounced faults.

(2) Repair is not taken into account in evaluting $(P_i)_{av}$, i.e., at subsystem testing a component is replaced "immediately" if faulty. Nor is unavailability due to testing itself taken into account since the test duration is short compared with the test interval τ_1, and, furthermore, only one subsystem is tested at a time.

(3) The components in A_2 and B_2 are assumed not to fail once activated on a demand for spraying. This is a reasonable assumption as these components are passive.

(4) The required operating time $t_0 \ll$ "mean time to on-line failure of subsystems A_1 and B_1". We therefore neglect the possibility of a system's failing more than once in t_0.

(5) The individual repair time distributions $Q_i(t)$ and $R_i(t)$ are calculated as a weighted sum of single component repair time distributions; the weighting is done with respect to the frequency of occurrence of component failures[6].

4.4. Evalution of P_u

$P_{A_1}(t)$, the probability that subsystem A_1

cannot be activated at itme t, can be calculated from knowledge of the point unavailability functions of the components in A_1.

Let $V_s(t)$ denote the probability that an unannounced failure of component V is present at time t after the component has been tested s times at intervals τ_1 and replaced if it has been found to be failed at any of these testings. $V_s(t)$, $t \geq s\tau_1$ can be determined from the recursion relation[7].

$$V_s(t) = V_{s-1}(s\tau_1) V_0(t - s\tau_1) + V_{s-1}(t) - V_{s-1}(s\tau_1), \quad (1)$$

i.e., by puttings$=1, 2, \cdots\cdots, n$, the variables can be calculated successively until $t=T=n\tau_1$, the lifetime of the plant. On the basis of the component "$V_s(t)$ – functions" evaluated from Eq. (1), $P_{A_1}(t)$ can be determined within each interval of time τ_1 by using the elementary addition and multiplication rules for probabilities. $P_{A2}(t)$, the probability that subsystem A_2 cannot be activated at time t, is calculated in a similar way.

The probability that system A cannot be activated at time t is[8]

$$P_A(t) = P_{A_1}(t) + P_{A2}(t) - P_{A_1}(t)\ P_{A2}(t) \text{ for } 0 \leq t \leq T \quad (2)$$

The mean unavailability of system A within the operating time of the plant is

$$(P_A)_{av} = \frac{1}{T}\int_0^T P_A(t)\, dt \quad (3)$$

$(P_B)_{av}$ is given by an analogous expression.

As a measure for the unavailability of the total spray system (A and B), we take the average probability of simultaneous failure of A and B within T

$$P_u = \frac{1}{T}\int_0^T P_A(t) P_B(t)\, dt \quad (4)$$

4.5. Evaluation of P_0 and P_s

Given a demand for containment spray at time t, Fig.3 identifies the event sequence

$a \equiv$ {A_2 is available; B_2 is not available; A_1 is available. but A_1 fails before $t+t_0$}

The probability of this sequence is

$$G_a(t) = \overline{P_{A2}(\cdot)}\, P_{B2}(t)\, \overline{P_{A1}(t)}\, F_{A_1}(to) \quad (5)$$

The $Pi(t)$ are usually very small so that $\overline{P_{A2}(\cdot)}\, P_{B2}(t)\, \overline{P_{A1}(\cdot)} \cong P_{B2}(t)$. By using this approximation and averaging $G_a(t)$ over the interval o to T, we obtain

$$(G_c)_{av} \cong (P_{B2})_{av} F_{A_1}(to) \quad (6)$$

The expression for $(G_b)_{av}$ is identical with Eq. (6) with subscripts A and B interchanged.

$$(G_b)_{av} \cong (P_{A2})_{av} F_{B_1}(to) \quad (7)$$

The event sequence c in Fig.3 is

$c \equiv$ {A_2 is available; B_2 is available; A_1 is available; B_1 is not available, But A_1 fails before B_1 is repaired}

The probability of this sequence given a demand at time t is

$$G_c(t) = \overline{P_{A2}(t)}\, \overline{P_{B2}(t)}\, \overline{P_{A1}(t)}\, P_{B1}(t) \int_0^{to} f_{A1}(t_1)\, \overline{Q_{B1}(t_1)}\, dt_1 \quad (8)$$

By the same manner we obtain

$$(G_c)_{av} \cong (P_{B1})_{av} \int_0^{to} f_{A1}(t_1)\, \overline{Q_{B1}(t_1)}\, dt_1 \quad (9)$$

The probability of event sequence d is identical with Eq. (8) with A_1 and B_1 interchanged.

Event sequence e is

$e \equiv$ {Subsystems A_2, B_2, A_1, B_1 are available, but A_1 fails,then B_1 fails before A_1 is repaired}

The probability of this sequence is

$$G_e(t) = \overline{P_{A2}(t)}\, \overline{P_{B2}(t)}\, \overline{P_{A1}(t)}\, \overline{P_{B1}(t)} \int_0^{to} \int_{t1}^{to} f_{A1}(t_1)\, f_{B1}(t_2) \times \overline{K_{A1}}(t_2 - t_1)\, dt_2 dt_1 \quad (10)$$

Averaging again over the interval 0 *to* T and keeping only the most dominant term, we get

$$(G_e)_{av} = \int_0^{to} f_{A_1}(t_1) \int_{t_1}^{to} f_{B1}(t_2)\, \overline{R_{A_1}}(t_2 - t_1)\, dt_2 dt_1 \quad (11)$$

$(G_f)_{av}$ is identical with Eq. (11) with A_1 and B_1 interchanged. The probability Po is then

$$Po = \sum_{i=a}^{f} (Gi)\, av \quad (12)$$

The probability for system failure, Ps is obtained by the sum of Pu and Po.

$$Ps=Pu+Po$$

Hence, the quantity Ps can be interpreted as the average probability of system failure given a demand for containment spray.

4.6. Numerical Example

Assuming the subsystems A_1, A_2, B_1 and B_2 consist of constant failure rates, we get

$$P_{A_1}(t)=P_{B_1}(t)=1-2\exp\{-(\lambda_1+\lambda_2)t\}+\exp\{-(\lambda_1+2\lambda_2)t\} \quad 0\le t<\tau_1 \tag{14}$$

$$P_{A2}(t)=P_{B2}(t)=1-\exp(-\lambda_3 t) \quad 0\le t<\tau_2 \tag{15}$$

$$F_{A_1}(t)=F_{A_1}(t)=1-2\exp\{-(\lambda_1+\lambda_2)t\}+\exp\{-(\lambda+2\lambda_2)t\} \tag{16}$$

where

λ_1=sum of failure rates of components connected in series in subsystem A_1 and B_1

λ_2=failure rates of redundant components in A_1 and B_1

λ_3=sum of failure rates of components connected in series in subsystem A_2 and B_2

In case of constant failure rates for the components, $P_{A_1}(t)$ is periodic with m periods within τ_2, and $P_{A2}(t)$ is periodic with the period τ_2. Therefore, $(P_A)_{av}$ can be calculated from Eqs. (2) and (3) with T replaced by τ_2

$$(P_A)_{av}=(P_B)_{av}=\frac{1}{\tau_2}\sum_{k=0}^{m-1}\int_{k\tau_1}^{(k+1)\tau_1}[1-2\exp\{-(\lambda_1+\lambda_2)(t-k\tau_1)-\lambda_3 t\}+\exp\{-(\lambda_1+2\lambda_2)(t-k\tau_1)-\lambda_3 t\}]dt \tag{17}$$

For $(\lambda_1\tau_1,\ \lambda_2\tau_1,\ \lambda_3\tau_2)\ll(1,1,1)$, the result is

$$(P_A)_{av}=(P_B)_{av}\cong\frac{1}{2}\lambda_1\tau_1+\frac{1}{2}\lambda_3\tau_2 \tag{18}$$

Similarly, from Eq. (4) with T replaced by τ_2, Pu, in the limit of small $\lambda_1\tau_1$, $\lambda_2\tau_1$, and $\lambda_3\tau_2$, can be approximated as Eq. (19)

$$Pu\cong\frac{1}{6}\lambda_1(2\lambda_1+\lambda_3)\tau_1^2+\frac{1}{2}\lambda_1\lambda_3\tau_1\tau_2+\frac{1}{3}\lambda_3^2\tau_2^2 \tag{19}$$

Eqs. (18) and (19) show that $(P_A)_{av}$ and Pu are constant with respect to λ_2 in case of $\lambda_2\tau_1\ll 1$.

Assuming that the repair times are constant, i.e.,

$$Q_{A1}(t)=Q_{B1}(t)=\begin{cases}0 & \text{for } 0\le t<T_1\\ 1 & \text{otherwise}\end{cases} \tag{20}$$

$$R_{A1}(t)=R_{B1}(t)=\begin{cases}0 & \text{for } 0\le t<T_2\\ 1 & \text{otherwise}\end{cases} \tag{21}$$

we find, in the limit of $(\lambda_1\tau_1,\ \lambda_2\tau_1,\ \lambda_3\tau_2)\ll(1,1,1)$,

$$(G_a)av=(G_b)av\cong\frac{1}{2}\lambda_3\tau_2\lambda_1 t_0 \tag{22}$$

$$(G_c)av=(G_d)av\cong\frac{1}{2}\lambda_1^2\tau_1 T_1 \tag{23}$$

$$(G_e)aa=(G_f)av\cong\lambda_1^2 T_2\left(t_0-\frac{1}{2}\lambda_1 t_0^2\right) \tag{24}$$

From Eq. (12),

$$Po\cong\lambda_3\tau_2\lambda_1 t_0+\lambda_1^2\tau_1 T_1+2\lambda_1^2 T_2\left(t_0-\frac{1}{2}\lambda_1 t_0^2\right) \tag{25}$$

For numerical example, failure rates of components are shown in Table 1[9]. The containment spray system must operate for half an hour after the postulated large LOCA incident. Technical specifications by the Nuclear Regulatory Commission (NRC) require that this system be tested once a month. A pressurized water reactor is operated for 11 months and then shutdown for refuelling for about a month. A thorough proof testing of the containment spray system is performed during this interval. Mean repair time is assumed to be 7.1 hours[9]. Therefore values of parameters are given as

$to=0.5$ hour $T_1=7.1$ hours $T_2=0.4$ hour

$\lambda_1=9.14\times10^{-5}$/hour $\lambda_2=1\times10^{-3}$/hour

$\lambda_3=1.3\times10^{-7}$/hour

$\tau_1=720$hours $\tau_2=7920$hours $m=11$

Now we can get values of Pu and Po by substituting above values into Eqs. (19) and (25), respectively.

$$Pu=1.4788\times10^{-3} \quad Po=4.2755\times10^{-5}$$

Thus, the probability that the containment

Table 1. Failure rates of components

Components	Failure rates (per hour)
Blockage of plugger in RWST	$1x10^{-10}$
Valves V_{1A}, V_{1B}	1×10^{-5}
Valves V_{2A}, V_{2B}	1×10^{-5}
Filters F_A, F_B	3×10^{-7}
Pumps P_A, P_B	3×10^{-5}
Valves V_{3A}, V_{4A}, V_{3B}, V_{4B}	1×10^{-6}
Valves V_{7A}, V_{7B}	1×10^{-7}
Nozzles S_A, S_B	3×10^{-3}
Loss of power	4.11×10^{-5}

spray system is unavailable, given a LOCA, is the sum of Pu and Po as Eq. (13).

$$Ps=1.5205\times10^{-3}$$

5. Concluding Remarks

For simplicity the human error and common mode failures are not included in this model; common mode failures caused for instance by missiles, temperature, pressure, humidity, or vibration influences during accident conditions are not usually amenable to mathematical approach.

The functional dependence of Ps on both τ_1 and τ_2 (Pu as well as Po depends on τ_1 and τ_2) suggests that Ps can be used in connection with planning of the test policy by studying the sensitivity of Ps under variation of the parameters τ_1 and τ_2.

We show that cause-consequence charts may be utilized as one of the tools for analysis and problem formulation. They provide a logical and perspicuous basis for qualitative as well as quantitative reliability analysis.

References

1. "An assessment of Accident Risks in U.S. Commercial Nuclear Power Plants" WASH-1400, United States Atomic Energy Commision, Reactor Safety Study, 1974.
2. E. Phibbs and S.H. Kuwamoto, "Fault-tree Analysis", IEEE Trans. on Reliability Vol. R-23, p. 226, Oct., 1974.
3. D.S. Nielsen, "The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis", Danish Atomic Energy Commission, Riso-M-1374, May. 1971.
4. R.G. Bennetts, "On the Analysis of Fault Trees", IEEE Trans. on Reliability Vol. R-24, No.3, pp. 175-184, August, 1975.
5. Final System Description, "Containment Spray System" in Ko-Ri Nuclear Power Plant.
6. D.S. Nielsen, and B. Runge, "Unreliability of a Standby System with Repair and Imperfect Switching", IEEE Trans. on Reliability, Vol. R-23, pp. 17-24, April, 1974.
7. E.R. Woodcode, "The Calculation of Reliability of Systems, The Program Noted," United Kingdom Atomic Energy Authority, AHSB(S) R 153, 1968.
8. M.L. Shooman, "Probabilitic Reliability: An Engineering Approach", Chapter 3. McGraw-Hill, Inc. 1968.
9. United States Nuclear Regulatory Commission, Appendix II, "PWR fault trees", in Reactor Safety Study. WASH-1400, 1975.