Journal of the Korean Nuclear Society
Volume 24, Number 1, March 1992

Development of a Computer Code for Common Cause Failure Analysis

Byung Hyun Park and Nam Zin Cho
Korea Advanced Institute of Science and Technology

(Received February 25, 1991)

공통원인 고장분석을 위한 전산 코드 개발

박병현 · 조남진
한국과학기술원

(1991. 2. 25 접수)

Abstract

COMCAF, a computer code for the common-cause failure analysis, is developed to treat the common-cause failures in nuclear power plants.

In the treatment of common-cause failures, the minimal cut sets of the system are obtained first without changing the fault-tree structure. The occurrence probabilities of the minimal cut sets are then calculated accounting for the common-cause failures among components in the same minimal cut set or in different minimal cut sets. The basic parameter model is used to model the common-cause failures between similar or identical components. For dissimilar components, the assumption of symmetry used in the basic parameter model is applied to the basic events affecting two or more components. The top event probability is evaluated using the inclusion-exclusion method. In addition to the common-cause failures of components in the same minimal cut sets, failures of components in the different minimal cut sets are also easily accounted for by this method.

This study applied this common-cause failure analysis to the PWR auxiliary feedwater system. The results in the top event probability for the system are compared with those of no common-cause failures.

요 약

원자력 발전소에서 발생하는 공통원인 고장을 분석하기 위한 컴퓨터 코드 COMCAF를 개발하였다.

공통원인 고장을 다룰 때, 먼저 계통의 최소 단절집합들을 공통원인 기본사상들이 고려되지 않은 고장수목으로 부터 구한다. 그리고, 공통원인 고장들이 같은 최소 단절집합내의 부품들간에 있는지 또는 서로 다른 최소 단절집합들의 부품들간에 있는지를 고려하여 이들 최소 단절집합들의 발생 확률값을 계산한다. 유사하거나 동일한 부품들간에 공통원인 고장이 있을때는 Basic Para-

meter 모델을 사용한다. 그러나, 서로 다른 부품들간에 공통원인 고장이 있을때는 Basic Parameter 모델에 쓰인 Symmetry Assumption을 두개 이상의 부품에 영향을 주는 기본사상들에만 적용한다. Inclusion-Exclusion 방법을 사용하여 정점사상 확률값을 구한다. 이 경우 같은 최소 단절집합들에 있는 부품들의 공통원인 고장뿐만아니라 서로 다른 최소 단절집합들에 있는 부품들의 공통원인 고장도 쉽게 고려될 수 있다.

본 연구에서는 이러한 공통원인 고장분석을 가압경수로의 보조 급수계통에 적용하였다. 이들 정점사상의 확률값들을 공통원인 고장이 없는 경우와 비교하였다.

1. Introduction

Many methods such as the beta factor model[1], binomial failure-rate model[2,3], and multiple greek letter model[4,5] have been proposed to describe the common-cause failures.

The beta factor model has been considered as a simple, useful and reliable model and it has been used extensively for quantitative analysis of common-cause failures in nuclear power plants. However, the beta factor model does not allow a distinction between different multiple-component failures. The binomial failure-rate model is a special case of the more general model developed by Marshall and Olkin[6]. The Marshall-Olkin model has been specialized for application when data are sparse[7]. It is assumed that the components a system are identical or at least similar, so that the failure rate depends only on the number of components failed. The multiple greek letter model is an extension of the beta factor model to systems with high level of redundancy[5]. This model is mathematically equivalent to the basic parameter model and produces the same results as the basic parameter model, given a consistent interpretation of the data in estimating parameters[8].

The objectives of this study are to investigate effects of the common-cause failures in different minimal cut sets and those of the common-cause failures within minimal cut sets in highly redundant systems and to develop a computer code for automating the analysis of these common-cause failures. If the rare event approximation is used, the common-cause failures between components within a minimal cut set can be easily accounted for, but the effects of the common-cause failures between components in the different minimal cut sets cannot be considered. However, these can be included by the inclusion-exclusion method[9].

2. Modeling of Common-Cause Failures

In general, dependent failures are grouped in two categories[10]. First, there are failures resulting from failure of a common support system, an operation error, or an external initiating event such as an earthquake, fire of flood, which can be modeled explicitly by building the dependence into the fault-tree and event-tree structure. This group of dependent failures is treated explicitly in the fault trees because it is possible to identify the cause and effect. The second group includes potential dependent failures resulting from many different root causes such as common manufacturer, common environment, maintenance error, etc., that have been handled by modifying minimal cut set probabilities to take into account dependent failures among groups of components. There are so many potential causes that an explicit representation of all of them in an event- or fault-tree would be intractable.

2.1. Definition and Types of Common-Cause Failures

Several terms have been used to describe specific types of dependent failures[11]. Common-cause failures are multiple, concurrent, and de-

pendent failures of identical components that fail in the same mode. Propagating failures occur when a component fails in a mode that causes sufficient changes in operating conditions, environments, or requirement to cause other components to fail. Common–cause failures are failures of multiple components occurring from some single cause that is common to all of them.

In this study, the term common–cause failure will be used to describe the effect of all multiple, concurrent, and dependent failures. There are two classes of common–cause failures[11] : those due to generic causes and those due to special conditions. The generic causes are defined as out–of–tolerance operating conditions ; the special conditions refer to conditions or attributes that may be common to a number of system components. These causes and conditions form the basis for search of common–cause failures.

2.2. Common–Cause Basic Events and Component Groups

According to the generic causes and special conditions, certain groups of components or all of components at the same situation may fail simultaneously. Specific groups of components are susceptible to the common causes because they are exposed to the same environments.

We can classify the common–cause components by some criteria[8]. For example, components should be in the same group when they are in a functionally redundant configuration, similar or identical, active, normally in the same mode of operation, normally exposed to similar internal and external environments, and designed to perform the same function at the same time. Components can be excluded from a common–cause component group when they are passive, diverse, normally operated in different modes ; e.g., operation versus standby, nonredundant, and in different functions.

For a system composed of m components, there exist 2^m-1 states of system failure which are represented by the state vector $\vec{x}_j$ for jth mode of failure state[6]. For example, if a system is composed of three components, we have 7 state vectors consisting of 0's for nonfailure and 1's for failure.

We define common–cause basic event as one that affects the system in some way. The system–failure state is determined as one of the above states by a single common–cause basic event if any cause occurs.

The notation for the common–cause basic events is provided for the common–cause component group of (a, b, c) as follows : (1) $X_{a,in}$, $X_{b,in}$, $X_{c,in}$: basic events affecting one component (independent events), (2) X_{ab}, X_{ac}, X_{bc} : basic events affecting two components, and (3) X_{abc} : basic event affecting all three components.

2.3. Marshall–Olkin Model and Basic Parameter Model

A general model for common–cause failures was developed by Marshall and Olkin[6]. The marshall–Olkin model assumes that each failure mode $\vec{x}$ has the exponential distribution function $f_{\vec{x}}(t)$ which is defined as follows :

$$f_{\vec{x}}(t) = \lambda_{\vec{x}} \exp(-\lambda_{\vec{x}} t) \qquad t \geq 0 \qquad (2.1)$$

where $\lambda_{\vec{x}}$ is a constant failure rate associated with the m–dimensional state vector $\vec{x}$.

The cumulative distribution function $F_{\vec{x}}(t)$ is given by

$$F_{\vec{x}}(t) = 1 - \exp(-\lambda_{\vec{x}} t) \qquad (2.2)$$

Eq. (2.2) can be approximated for a small value of $\lambda_{\vec{x}} t$ as follows :

$$F_{\vec{x}}(t) \simeq \lambda_{\vec{x}} t \qquad (2.3)$$

The probability of common–cause basic event X of the system failure state vector $\vec{x}$ which is pro-

vided by Eq. (2.3) is also denoted by the notation Q.

For example, for a common-cause component group of 3 components, component failure events are given in terms of the basic events as follows:

$$X(a) = X_{a,in} \cup X_{ab} \cup X_{ac} \cup X_{abc} \quad (2.4a)$$

$$X(b) = X_{b,in} \cup X_{ab} \cup X_{bc} \cup X_{abc} \quad (2.4b)$$

$$X(c) = X_{c,in} \cup X_{ac} \cup X_{bc} \cup X_{abc} \quad (2.4c)$$

$$X(a)X(b) = X_{a,in}X_{b,in} \cup X_{ab} \cup X_{abc} \cup X_{a,in}X_{bc} \cup X_{b,in}X_{ac} \quad (2.4d)$$

$$X(a)X(c) = X_{a,in}X_{c,in} \cup X_{ac} \cup X_{abc} \cup X_{a,in}X_{bc} \cup X_{c,in}X_{ab} \quad (2.4e)$$

$$X(b)X(c) = X_{b,in}X_{c,in} \cup X_{bc} \cup X_{abc} \cup X_{b,in}X_{ac} \cup X_{c,in}X_{ab} \quad (2.4f)$$

$$X(a)X(b)X(c) = X_{a,in}X_{b,in}X_{c,in} \cup X_{abc} \cup X_{a,in}X_{bc} \cup X_{b,in}X_{ac} \cup X_{c,in}X_{ab} \quad (2.4g)$$

and the probabilities of component failure events are given in terms of the probabilities of the common-cause basic events as follows:

$$\Pr[X(a)] = Q_{a,in} + Q_{ab} + Q_{ac} + Q_{abc} \quad (2.5a)$$

$$\Pr[X(b)] = Q_{b,in} + Q_{ab} + Q_{bc} + Q_{abc} \quad (2.5b)$$

$$\Pr[X(c)] = Q_{c,in} + Q_{ac} + Q_{bc} + Q_{abc} \quad (2.5c)$$

$$\Pr[X(a)X(b)] = Q_{a,in}Q_{b,in} + Q_{ab} + Q_{abc} + Q_{a,in}Q_{bc} + Q_{b,in}Q_{ac} \quad (2.5d)$$

$$\Pr[X(a)X(c)] = Q_{a,in}Q_{c,in} + Q_{ac} + Q_{abc} + Q_{a,in}Q_{bc} + Q_{c,in}Q_{ab} \quad (2.5e)$$

$$\Pr[X(b)X(c)] = Q_{b,in}Q_{c,in} + Q_{bc} + Q_{abc} + Q_{b,in}Q_{ac} + Q_{c,in}Q_{ab} \quad (2.5f)$$

$$\Pr[X(a)X(b)X(c)] = Q_{a,in}Q_{b,in}Q_{c,in} + Q_{abc} + Q_{a,in}Q_{bc} + Q_{b,in}Q_{ac} + Q_{c,in}Q_{ab} \quad (2.5g)$$

The Marshall-Olkin model has so many basic events that it is difficult to describe the component failure events explicitly such as the above equations for large values of m.

The basic parameter model takes advantage of the assumption of symmetry. The assumption of symmetry[12] implies that the frequency of each basic event depends only on the number of affected components, not on the specific combination. This assumption of symmetry also can be expressed such that the probability of all common-cause basic events affecting the same number of components is equal. This assumption is reasonable if components in a common-cause group are identical or similar. In a three component system, this is applied as

$$Q_1 = \Pr(X_{a,in}) \simeq \Pr(X_{b,in}) \simeq \Pr(X_{c,in}) \quad (2.6a)$$

$$Q_2 = \Pr(X_{ab}) \simeq \Pr(X_{ac}) \simeq \Pr(X_{bc}) \quad (2.6b)$$

$$Q_3 = \Pr(X_{abc}) \quad (2.6c)$$

where Q_1, Q_2, and Q_3 are called the basic parameters.

By this assumption, the number of parameters to estimate are reduced from 2^m-1 in the Marshall-Olkin model to m in the basic parameter model. For the common-cause component group having 3 components, Eqs. (2.5a~g) also are approximated as follows:

$$\Pr[X(a)] \simeq Q_1 + 2Q_2 + Q_3 \quad (2.7a)$$

$$\Pr[X(b)] = \Pr[X(c)] = \Pr[X(a)] \quad (2.7b)$$

$$\Pr[X(a)X(b)] \simeq Q_1^2 + Q_2 + Q_3 + 2Q_1Q_2 \quad (2.7c)$$

$$\Pr[X(a)X(c)] = \Pr[X(b)X(c)] = \Pr[X(a)X(b)] \quad (2.7d)$$

$$\Pr[X(a)X(b)X(c)] \simeq Q_1^3 + Q_3 + 3Q_1Q_2 \quad (2.7e)$$

In the basic parameter model, the number of equations for the component failures as well as the parameters for the basic events are reduced from 2^m-1 to m.

2.4. Parameter Estimation

In PRA systems analysis, there are two different forms of data available to the analyst : parametric data and event data. The parametric data mean the numerical data that quantify the parameters of a model. Ideally, these data are based, at least in part, on event data, i.e., reports of operating experiences that are systematically collected. To perform a meaningful common-cause analysis, it is imperative that the process of the parameter estimation be properly integrated into the system model. This requires that the event reports be integrated and classified in a manner consistent with the assumptions built into the models.

The parametric common-cause analysis approach requires event data to be classified and categorized prior to parameter estimation. The basic parameter model requires, first, that each event be categorized as an independent or dependent event and, second, that the dependent event be assessed according to its impact on the collection of the components in its common-cause group. For the basic parameter model, the impact is measured in terms of a probability distribution on the number of failed components[12].

To develop estimators for the parameters of the basic parameter model, we start with the following general formula for the total component failure frequency Q_t of a given failure mode of a component in a system of m (identical and redundant) components

$$Q_t \simeq \sum_{k=1}^{m} \frac{(m-1)!}{(m-k)!(k-1)!} Q_k \qquad (2.8)$$

where Q_k is the frequency of simultaneous failure of k components in the system.

The maximum likelihood estimator for Q_k is

$$\hat{Q}_k = n_k \Big/ \left(\frac{m!}{(m-k)!k!} N_D \right) \qquad k = 1, \cdots, m \qquad (2.9)$$

where n_k is the number of events involving k components in failed state, and N_D is the number of demands on the entire system of m components.

Eq. (2.9) assumes that the data are collected from a set of N_D system demands in which the performance of all m components in the common-cause group are checked. Similar estimators can be developed for rate of failure per unit time by replacing N_D with T, the total system operating time. It is important to note that because of Eq. (2.9), the parameters of the basic parameter model are dependent on system size, m. Therefore, it is inappropriate to apply the parameters of the basic parameter model developed for one system size to te other system size.

Replacing Q_k in Eq. (2.8) with the maximum likelihood estimator in Eq. (2.9) yields

$$\hat{Q}_t \simeq \frac{1}{mN_D} \sum_{k=1}^{m} k n_k \qquad (2.10)$$

3. System Modeling for Common-Cause Failures

An objective of risk assessment is to determine the susceptibility of a system to conditions of design, operation, test, and maintenance that could lead to failure. This objective can be realized through system modeling for which a variety of analytical techniques can be used. The technique should produce a model that promotes understanding of the principal ways in which the system can fail and the ways in which the system can fail due to common causes and the ways in which the common-cause failures can be prevented or their impact reduced.

The fault tree analysis is one of the best available analytical tools for understanding how a sys-

tem works and might fail.

3.1. Fault Tree Analysis of Common-Cause Failures

The purpose of fault tree analysis is to find the fault event combinations that would occur with high probability. This is usually done by finding the smallest combinations of undesired state or event to occur. This undesired event described as the top event in the fault tree. The smallest combinations of fault events that cause the top event are the minimal cut sets. It is these minimal cut sets that form the bases for the evaluation of all plant ans system models.

In this study, the minimal cut sets are found first prior to the consideration of the common-cause failures. The effects of common-cause failures are then included during the quantitative evaluation of the minimal cut sets and the system failure probability. The events in the minimal cut sets are evaluated by Eqs. (2.4.a~g). In this manner, we express all the common-cause failure events by the equations. This "post-fault tree" approach of the common-cause failure analysis prevents the system fault tree from becoming huge and complex. The analysis of huge and complex fault tree not only requires large computation time but also may result in omission of important failure events during cut set generation due to truncation.

3.2. Top Event Probability : The Inclusion-Exclusion Method

Top event probability for a system composed of N minimal cut sets is given by[12]

$$\Pr(Top) = \Pr\left(\coprod_{i=1}^{N}\left(\prod_{j=1}^{K_i} X_{ij}\right)\right) \qquad i = 1,\cdots,N \tag{3.1}$$

where the event X_{ij} represents the jth event in the ith minimal cut set.

To account for all common-cause failure in the same or in the different minimal cut sets, we use the inclusion-exclusion method which provides successively upper and lower bounds on the top event probability which usually converge to the exact top event probability[9]. Let

$$S_k = \sum_{1\le i_1<i_2<\cdots<i_k\le N} \Pr(C_{i_1}\cap C_{i_2}\cap \cdots\cap C_{i_k}) \qquad k = 1,\cdots,N \tag{3.2}$$

Then the top event probability is given by

$$\Pr(Top) = \sum_{k=1}^{N}(-1)^{k-1}S_k \tag{3.3}$$

and bounds on the top event probability are given by

$$\Pr(Top) \le S_1 \tag{3.4a}$$

$$\Pr(Top) \ge S_1 - S_2 \tag{3.4b}$$

$$\Pr(Top) \le S_1 - S_2 + S_3 \tag{3.4c}$$

$$\vdots$$

In practice it may be necessary to calculate only a few S_k's to obtain a close approximation.

3.3. Example System

The example system is a stereo hi-fi system[9] with the following components : (a) FM tuner, (b) Record changer, (c) Amplifier, (d) Speaker A, and (e) Speaker B.

The system diagram is illustrated in Fig. 3.1. The number of minimal cut sets in this example system are 3, i.e., C_1=*(a, b)*, C_2=*(c)*, and C_3=*(d, e)*

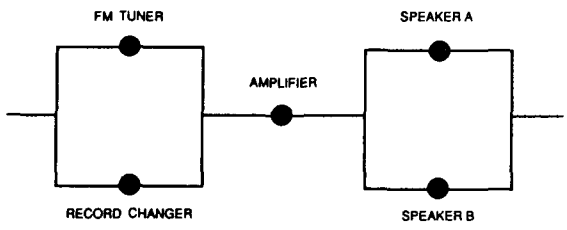

Fig. 3.1 The stereo hi–fi system

If all components in this system are independent of each other, then from Eq.(3.1) the top event probability is given by

$$\Pr(Top) = \Pr(C_1 \cup C_2 \cup C_3) = S_1 - S_2 + S_3 \quad (3.5)$$

where

$$S_1 = \Pr(C_1) + \Pr(C_2) + \Pr(C_3) = Q_{a,in}Q_{b,in} + Q_{c,in} + Q_{d,in}Q_{e,in} \quad (3.6a)$$

$$S_2 = \Pr(C_1C_2) + \Pr(C_1C_3) + \Pr(C_2C_3) = Q_{a,in}Q_{b,in}Q_{c,in} + Q_{a,in}Q_{b,in}Q_{d,in}Q_{e,in} + Q_{c,in}Q_{d,in}Q_{e,in} \quad (3.6b)$$

$$S_3 = \Pr(C_1C_2C_3) = Q_{a,in}Q_{b,in}Q_{c,in}Q_{d,in}Q_{e,in} \quad (3.6c)$$

If there exist dependences between components, the equation for the top event probability has the same form as Eq. (3.5) but its value is different from Eq. (3.5) because the values for S_i's should account for the terms due to the common–cause events.

When the common–cause component group consists of 3 components, we group the components such as (*b, c, d*). Then the following equations are developed :

$$S_1 = Q_{a,in}(Q_{b,in} + Q_{bc} + Q_{bd} + Q_{bcd}) + (Q_{c,in} + Q_{bc} + Q_{cd} + Q_{bcd}) + (Q_{d,in} + Q_{bd} + Q_{cd} + Q_{bcd})Q_{e,in} \quad (3.7a)$$

$$S_2 = Q_{a,in}(Q_{b,in}Q_{c,in} + Q_{bc} + Q_{bcd} + Q_{b,in}Q_{cd} + Q_{c,in}Q_{bd}) + Q_{a,in}(Q_{b,in}Q_{d,in} + Q_{bd} + Q_{bcd} + Q_{b,in}Q_{cd} + Q_{d,in}Q_{bc})Q_{e,in} + (Q_{c,in}Q_{d,in} + Q_{cd} + Q_{bcd} + Q_{c,in}Q_{bd} + Q_{d,in}Q_{bc})Q_{e,in} \quad (3.7b)$$

$$S_3 = Q_{a,in}(Q_{b,in}Q_{c,in}Q_{d,in} + Q_{bcd} + Q_{b,in}Q_{cd} + Q_{c,in}Q_{bd} + Q_{d,in}Q_{bc})Q_{e,in} \quad (3.7c)$$

If we use the basic parameters of the basic parameter model, the equations for the S_i's are very simplified. We can express Eq. (3.7*a*~*c*) as follows :

$$S_1 = 2Q_1(Q_1 + 2Q_2 + Q_3) + (Q_1 + 2Q_2 + Q_3) \quad (3.8a)$$

$$S_2 = 2Q_1(Q_1^2 + Q_2 + Q_3 + 2Q_1Q_2) + Q_1^2(Q_1^2 + Q_2 + Q_3 + 2Q_1Q_2) \quad (3.8b)$$

$$S_3 = Q_1^2(Q_1^3 + Q_3 + 3Q_1Q_2) \quad (3.8c)$$

4. Description of the Code COMCAF

COMCAF, a computer code for the COMmon–CAuse Failure analysis, was developed in this study to calculate the system failure probability of the system with dependences between components. The model for the common–cause failures is mainly the basic parameter model, but if the differences in component failure rates of the components in the common–cause group are large, the Marshall–Olkin model is modified to account for them.

4.1. Input and Output of the Code

COMCAF requires the minimal cut stes of the system as input for the calculation of the top event probability. The minimal cut sets are generated by the FTAP code[13]. The failure data are given as the total component failure rate for all

components in the system. When the experience data are available, we can generate the parameters using Eq. (2.10). The flow chart of COMCAF are illustrated in Fig. 4.1.

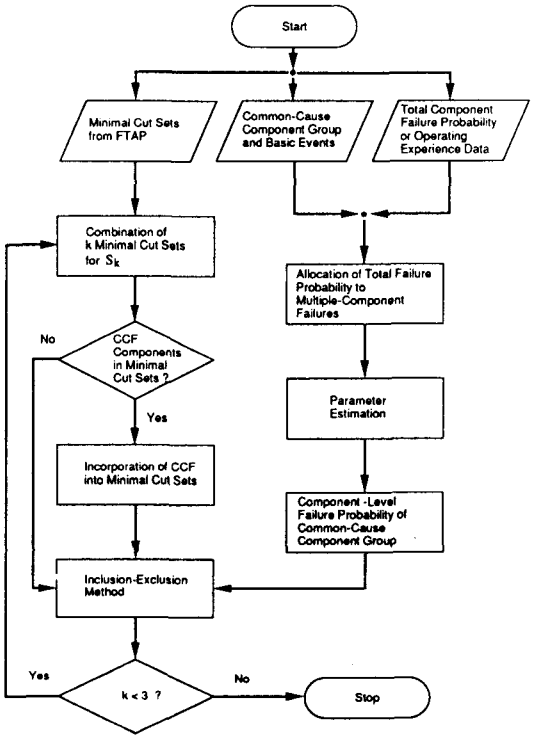

Fig. 4.1. Flow Chart of COMCAF

The input for common–cause component groups is composed of the components of the group and the failure rates for the basic events. This study allocates the common–cause percentage in the total component failure rate such that, for example, if the common–cause group of 3 components have 10% common–cause failure rate, the total component failure rate consists of 90% independent failure rate, 9% common–cause failure rate of two components failed and 1% common–cause failure rate of three components failed. This allocation of common–cause failure rate is arbitrary and modified correctly if the operating experience data are sufficient.

The parameters of the basic parameter model are calculated from Eq. (2.8) for the common–cause component group of m components as follows :

$$Q_k = \alpha_k Q_t \Big/ \left(\frac{(m-1)!}{(m-k)!(k-1)!} \right)$$

$$k = 1, \cdots, m \tag{4.1}$$

where α_k is the percentage of the failure rate involving k components in the total failure rate Q_t. If the operating experience data are provided, the parameters of the basic parameter model is given by Eq. (2.9).

4.2. Model of Common–Cause Failures

The basic parameter model is used for the incorporation of the common–cause basic events into the minimal cut sets. The assumption of symmetry in the basic parameter model is appropriate for an identical or similar components.

However, components are grouped in the same component group although their failure rates are different. In this case, the general Marshall–Olkin model is modified to account for the differences in the failure rates. Because the independent failure rate of a component is usually dominant in the total failure rate of a component, the difference is mainly due to this term. However, the common–cause failure terms are similar for all components in the common–cause component group. Therefore, the probability of the basic event for the independent failure is given for each component. Eqs. (2.5a~g) for the common–cause component group of 3 are modified as follows :

$$\Pr[X(a)] \simeq Q_{a,in} + 2Q_2 + Q_3 \tag{4.2a}$$

$$\Pr[X(b)] \simeq Q_{b,in} + 2Q_2 + Q_3 \tag{4.2b}$$

$$\Pr[X(c)] \simeq Q_{c,in} + 2Q_2 + Q_3 \tag{4.2c}$$

$$\Pr[X(a)X(b)] \simeq Q_{a,in}Q_{b,in} + Q_2 + Q_3 + Q_{a,in}Q_2 + Q_{b,in}Q_2 \tag{4.2d}$$

$$\Pr[X(a)X(c)] \simeq Q_{a,in}Q_{c,in} + Q_2 + Q_3 + Q_{a,in}Q_2 + Q_{c,in}Q_2 \quad (4.2e)$$

$$\Pr[X(b)X(c)] \simeq Q_{b,in}Q_{c,in} + Q_2 + Q_3 + Q_{b,in}Q_2 + Q_{c,in}Q_2 \quad (4.2f)$$

$$\Pr[X(a)X(b)X(c)] \simeq Q_{a,in}Q_{b,in}Q_{c,in} + Q_3 + Q_2(Q_{a,in} + Q_{b,in} + Q_{c,in}) \quad (4.2g)$$

4.3. Calculation of Top Event Probability

If we retain only the first term in Eq. (3.3), i.e., S_1, the top event probability is the rare event approximation given by

$$\Pr(Top) \simeq \sum_{i=1}^{N} \Pr\left(\prod_{j=1}^{K_i}(X_{ij})\right) \quad (4.3)$$

The rare event approximation provides the consideration of the common-cause failures between components in the same minimal cut sets. However, it cannot account for the common-cause failure between components in the different minimal cut sets. We can overcome this limitation by expanding a few more terms in Eq. (3.3) for the top event probability. In this study we consider the first three terms in Eq. (3.3). Thus, we evaluate the system failure frequency conservatively as follows :

$$\Pr(Top) \simeq S_1 - S_2 + S_3 \quad (4.4)$$

If we apply S_1 in Eq. (4.3) for the calculation of top event probability without changing the occurrence probability of the minimal cut sets in Eq. (4.2), the top event probability is overestimated because the same common-cause basic event appears several times. Therefore, S_1 is modified by deleting the repeatedly-occurring supersets of the common-cause basic events and this is denoted by S_1^*. The results of S_1^* are compared to those of FTAP.

5. Applications to Auxiliary Feedwater System

The auxiliary feedwater system(AFWS) supplies, in the event of a loss of the main feedwater supply, sufficient feedwater to the steam generators to remove residual core energy (decay heat) stored in the primary system. The AFWS has a highly redundant configurations of the components in the delivery of the feedwater. The CCF analyses for the AFWS are performed by COMCAF and FTAP code using the different approaches in the calculation of the system failure probability and the results are compared with each other.

5.1. Description of Auxiliary Feedwater System

The AFWS is shown in Fig. 5.1[14]. Except for the common supply line from the codensate storage tanks, the two reactor units have separate AFWS. The AFWS has two electric-motor-driven pumps and one turbinedriven pump. Each of the electric pumps serves two steam generators and the turbine pump serves all four steam generators.

The AFWS provides complete redundancy in pump capacity and water supply for all cases for which the system is required. Only two steam generators are required to be usable for any credible accident condition. Redundant electrical power and air supplies assure reliable system initiation and operation. The electric-motor-driven pumps are powered by offsite and onsite sources and the turbine-driven pump takes steam from either of the two main steam lines.

The AFWS consists of two subsystems. One subsystem utilizes a steam turbine-driven pump, with the steam capable of being supplied from No. 1 or No. 4 steam generator upstream of the main steam isolation valves. The other subsystem utilizes two motor-driven pumps. The discharge piping is arranged so that each pump supplies two steam generators.

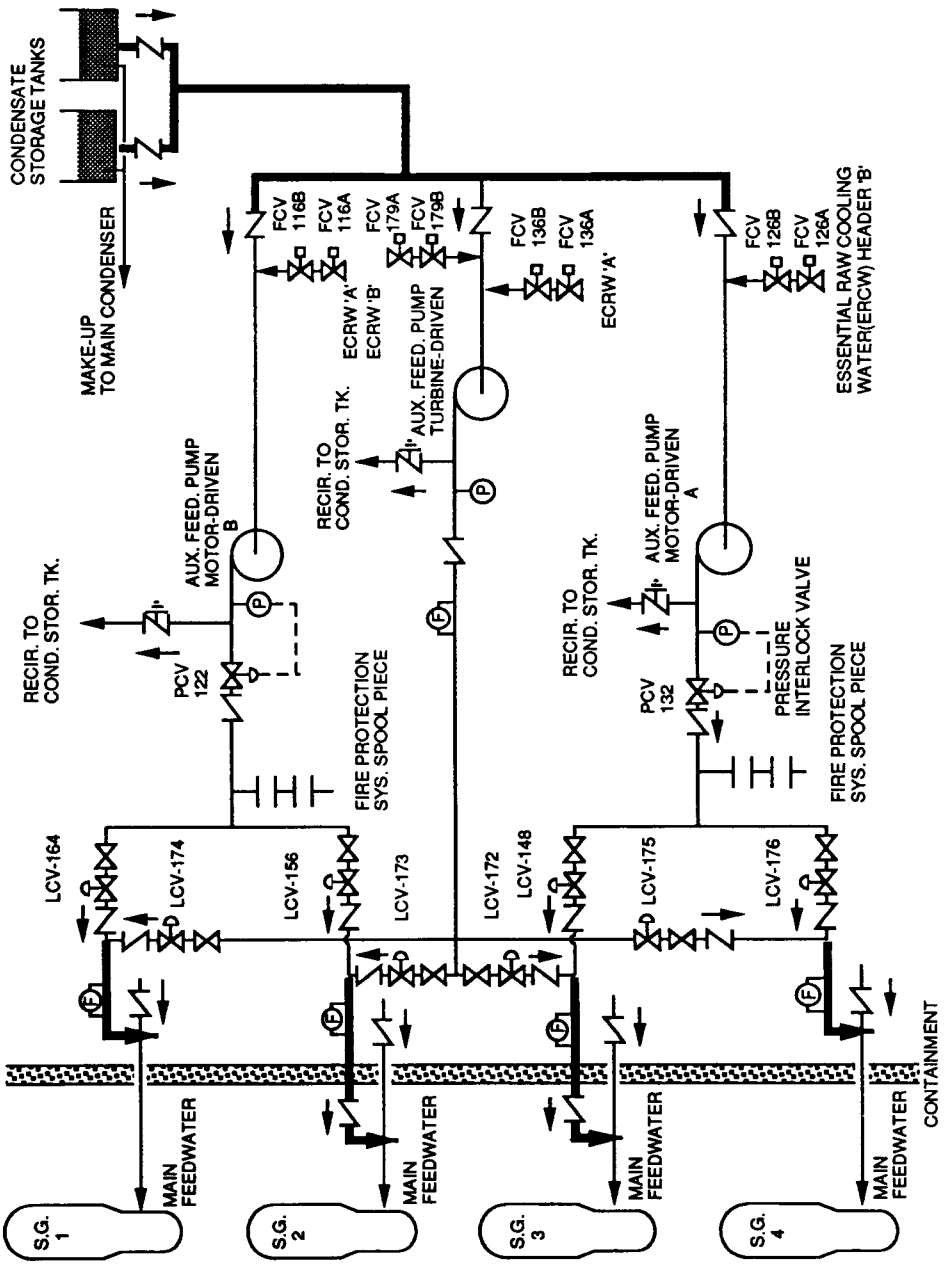

Fig. 5.1. Auxiliary Feedwater System

5.2. Input Data of Common-Cause Component Group

The failure data for PWR auxiliary feedwater systems are from Korea Nuclear Unit 1 (KNU-1) [15]. Its fault tree consists of 115 basic events. The 79 minimal cut sets are generated under the condition of cut-off value with 10^{-8} by the FTAP code. They cosist of 35 events of which failure data are shown in Table 5.1.

This study evaluates the system failure probability for the two distinct cases of the common-cause component groups. One is the component groups in which the components of common-cause failures are in the same minimal cut sets. The other is the component groups in which the components of common-cause failure are in the different minimal cut sets. The common-cause component groups having components in the same minimal cut set are shown in Table 5.2 according to the number of components in the group. Similarly, the common-cause component groups having components in the different minimal cut sets are shown in Table 5.3.

Table 5.2. Common-Cause Component Groups Having Components in the Same Minimal Cut Sets

Group	Events in Group(m=2)
1	VFE32AD, VFE32AC
2	VFE30AY, VFE30AC
3	COMIFVY, IFV503C
4	VFE29AY, VFE29AC
5	VFE32BD, VFE32BC
6	VFE30BY, VFE30BC
7	VFE29BY, VFE29BC
8	COMSIGF, IFV504C

Table 5.1. Failure Data in AFWS

Event I.D.	Failure Probability	Event I.D.	Failure Probability
VFE32AD	1.00×10^{-4}	VFE30BY	1.00×10^{-4}
VFE32AC	1.00×10^{-4}	VFE30BC	1.00×10^{-4}
VFE30AY	1.00×10^{-4}	VFV504C	1.00×10^{-4}
VFE30AC	1.00×10^{-4}	IFV504Y	7.53×10^{-3}
COMIFVY	3.00×10^{-5}	VFE29BY	1.00×10^{-4}
IFV503C	1.00×10^{-4}	VFE29BC	1.00×10^{-4}
IFV503Y	7.53×10^{-3}	VFE-4BD	1.00×10^{-3}
VFE29AY	1.00×10^{-4}	XPP30BA	1.00×10^{-3}
VFE29AC	1.00×10^{-4}	XPP30BY	7.90×10^{-3}
VFE-4AD	2.00×10^{-3}	CKPM3BF	1.00×10^{-3}
XPP30AA	1.00×10^{-3}	STPM3BT	4.00×10^{-3}
XPP30AY	7.90×10^{-3}	XPP-58A	1.00×10^{-2}
CKPM3AF	1.00×10^{-3}	XPP-58Y	7.90×10^{-3}
STPM3AT	4.00×10^{-3}	AFSIGAF	7.00×10^{-3}
TKCONDF	1.00×10^{-4}	AFSIGBF	7.00×10^{-3}
TKFRESF	5.00×10^{-3}	COMSIGF	1.20×10^{-6}
VFE32BD	1.00×10^{-4}	MAMSIGX	1.00×10^{-2}
VFE32BC	1.00×10^{-4}		

Table 5.3. Common-Cause Component Groups Having Components in the Different Minimal Cut Sets

Group	Events in Group(m=2)
1	COMSIGF, MAMSIGX
2	TKCONDF, TKFRESF
3	CKPM3BF, AFSIGAF
4	XPP30BA, VFE-4AD
5	STPM3AT, STPM3BT
6	IFV503Y, IFV504Y
7	XPP30AY, XPP-58A
8	XPP-58Y, XPP30BY

5.3. Results

This study considers two different cases for the common-cause failures. For each case, we obtain results and compare them with the system failure probability which is evaluated assuming all components are independent. We consider the common-cause component groups having the components in the different minimal cut sets. The system failure probabilities for the common-cause component groups of m=2 are shown in Fig. 5.2.

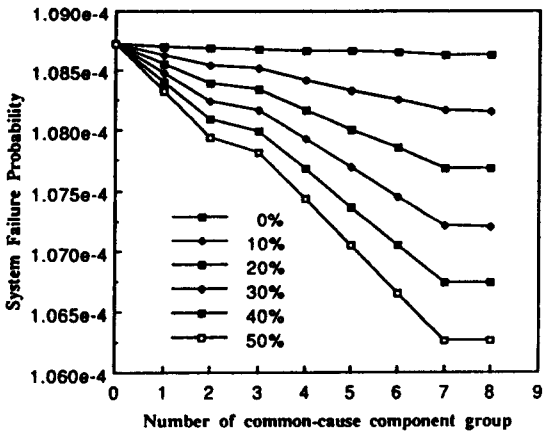

Fig. 5.2. The System Failure Probability for Components in the Different Minimal Cut Sets (m=2)

We also consider the common-cause component groups having components in the same minimal cut sets. The system failure probabilities obtained for m=2 by changing the percentage of the common-cause failure are shown in Fig. 5.3.

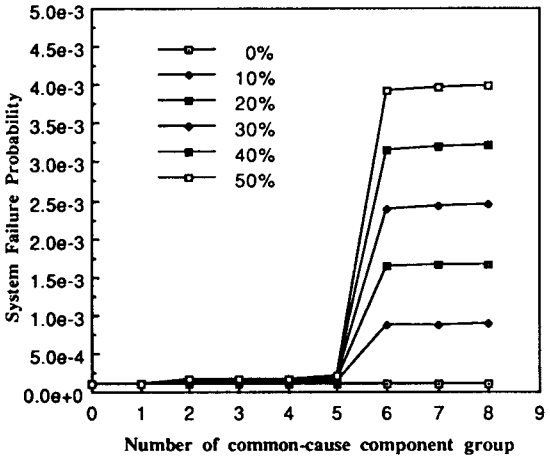

Fig. 5.3. The System Failure Probability for Components in the Same Minimal Cut Sets (m =2)

The CPU time and the system failure probability by COMCAF are compared with those by FTAP. The components of the common-cause component groups in Table 5.4 are used. First, the common-cause basic events for these components are incorporated explicitly into the fault tree. Then the minimal cut sets and the system failure probability for this new fault tree are obtained from FTAP. To compare the system failure probability by COMCAF with that by FTAP, S_1 in the exclusion-inclusion method of COMCAF is modified to become the same expression for the rare event approximation of FTAP.

The increase in the number of minimal cut sets under the cut-off with 10^{-8} and 10^{-10} is shown in Tables 5.5 and 5.6, respectively. The number of minimal cut sets increases significantly when the number of components of the common-cause failures increases. However, the increase changes depending on the cut-off value of FTAP.

Table 5.4. Common-Cause Component Groups Having Components in the Same Minimal Cut Sets-CASE 1,2,3

CASE 1

Group	Events in Group(m=2)
1	XPP30AY, XPP-58A
2	AFSIGAF, XPP30BY
3	STPM3AT, AFSIGBF
4	STPM3BT, XPP-58Y
5	VFE-4AD, IFV503Y
6	VFE29AY, IFV504Y

CASE 2

Group	Events in Group(m=3)
1	XPP30AY, XPP30BY, XPP-58A
2	AFSIGBF, IFV503Y, MANSIGX
3	STPM3AT, IFV504Y, XPP-58Y

CASE 3

Group	Events in Group(m=2)
1	IFV503Y, IFV504Y
2	TKCONDF, TKFRESF
3	COMSIGF, MANSIGX

Table 5.5. Comparisons of FTAP and COMCAF under Cut-Off with 10^{-8}-Increase in the Number of Basic Events and MCS' by FTAP

	# of Basic Events	# of MCS'
Withot CCF	115	79
Case 1	121	149
Case 2	127	237
Case 3	118	81

The CPU time of COMCAF is composed of the CPU time for the generation of the minimal cut sets from FTAP and the CPU time for the calculation of the system failure probability from COMCAF. The comparisons of the CPU time of FTAP and COMCAF under the cut-off with 10^{-8} and

Table 5.6. Comparisons of FTAP and COMCAF under Cut-Off with 10^{-8}-Increase in the Number of Basic Events and MCS' by FTAP

	# of Basic Events	# of MCS'
Withot CCF	115	611
Case 1	121	804
Case 2	127	879
Case 3	118	608

10^{-10} are presented in Tables 5.7 and 5.8, respectively. The CPU time of COMCAF is insensitive to the number of components in the common-cause component groups and the number of common-cause component groups. However, the CPU time of FTAP increases as the number of components of the common-cause failures increases.

Table 5.7. Comparisons of FTAP and COMCAF under Cut-Off with 10^{-8}-Comparison of CPU Time (in seconds)

	FTAP	COMCAF
Withot CCF	7.6	7.7
Case 1	10.1	7.7
Case 2	12.9	7.7
Case 3	8.3	7.7

Table 5.8. Comparisons of FTAP and COMCAF under Cut-Off with 10^{-8}-Comparison of CPU Time (in seconds)

	FTAP	COMCAF
Withot CCF	35.1	35.9
Case 1	43.0	36.1
Case 2	53.7	36.1
Case 3	34.1	36.0

The system failure probability by FTAP is calculated from the minimal cut sets which are generated from the new fault tree. The system failure probability by COMCAF is calculated by changing the occurrence probability of the minimal cut sets

which are generated from the fault tree without the common-cause failures. The comparisons of the system failure probability under the cut-off with 10^{-8} and 10^{-10} are shown in Tables 5.9 and 5.10, respectively.

Table 5.9. Comparisons of FTAP and COMCAF under Cut-Off with 10^{-8}-Comparison of System Failure Probability

	FTAP	COMCAF
Withot CCF	1.0872×10^{-4}	1.0872×10^{-4}
Case 1	1.5746×10^{-4}	1.5727×10^{-4}
Case 2	3.2234×10^{-4}	3.3932×10^{-4}
Case 3	8.5638×10^{-4}	8.5847×10^{-4}

Table 5.10. Comparisons of FTAP and COMCAF under Cut-Off with 10^{-10}-Comparison of System Failure Probability

	FTAP	COMCAF
Withot CCF	1.1043×10^{-4}	1.1043×10^{-4}
Case 1	1.5917×10^{-4}	1.6046×10^{-4}
Case 2	3.2410×10^{-4}	3.4277×10^{-4}
Case 3	8.5808×10^{-4}	8.5816×10^{-4}

The CPU time and the system failure probability of modified S_1 calculation of COMCAF given above are compared with those of COMCAF which include three terms of the inclusion-exclusion method under the cut-off with 10^{-8}. The comparisons of the CPU time and the system failure probability are given in Tables 5.11 and 5.12, respectively.

Table 5.11. Comparisons of S_1^* and $S_1-S_2+S_3$ by COMCAF under Cut-Off with 10^{-8}-Comparison of CPU Time(in seconds)

	S_1^*	$S_1-S_2+S_3$
Withot CCF	7.7	25.6
Case 1	7.7	63.9
Case 2	7.7	59.1
Case 3	7.7	51.2

*Modified S_1 calculation

Table 5.12. Comparisons of S_1^* and $S_1-S_2+S_3$ by COMCAF under Cut-Off with 10^{-8}-Comparison of System Failure Probability

	S_1^*	$S_1-S_2+S_3$
Withot CCF	1.0872×10^{-4}	1.0841×10^{-4}
Case 1	1.5727×10^{-4}	1.3833×10^{-4}
Case 2	3.3932×10^{-4}	2.5758×10^{-4}
Case 3	8.5847×10^{-4}	8.5734×10^{-4}

*Modified S_1 calculation

6. Summary

This study developed a method for the common-cause failure analysis that does not include common-cause events in the fault tree explicitly. The minimal cut sets are obtained from fault-tree which does not contain any common-cause failures. The component-level failure events and their probabilities are generated for each common-cause component groups. The probabilities of the minimal cut sets are then calculated using these component-level failure probabilities and these are used to calculate the system failure probability by the inclusion-exclusion method. The system failure probabilities are evaluated for different conditions of common-cause failures.

For common-cause failures between components in the different minimal cut sets, the system failure probabilities decrease considerably depending on the structure of the system fault tree and common-cause component group. As the number of common-cause component groups increases, the system failure probabilities tend to decrease. For a fixed number of common-cause component groups, the decrease in the system failure probability is larger when the number of components in the common-cause component groups is smaller.

For common-cause failures between components in the same minimal cut sets, the system

failure probabilities increase significantly for a certain common–cause component group. As the number of common–cause groups increases, the system failure probabilities also tend to increase significantly. For a fixed number of common–cause component groups, the increase in the system failure probability is larger when the number of components in the common–cause component groups is smaller.

Nomenclature

$\Pr(X)$: Probability of Event X
$X(a)$: Failure Event of Component a
$X_{a,in}$: Independent Failure Event of Component a
X_{ab} : Dependent Failure Event of Component a and Component b
X_{ij} : The jth Event in the ith Minimal Cut Set
$\vec{x}$: System State Vector
$f(t)$: Probability Distribution Function
$F(t)$: Cumulative Distribution Function
λ : Component Failure Rate
Q_a : Failure Frequency of Component a
$Q_{a,in}$: Independent Failure Frequency of Component a
Q_{ab} : Dependent Failure Frequency of Component a and Component b
Q_k : Failure Frequency of k Components
m : Number of Components in Common–Cause Component Group
n_k : Number of Events in which k Components are in Failed State
N_D : Nomber of Demands
Top : Top Event
C_i : The ith Minimal Cut Set
N : Number of Minimal Cut Sets
K_i : Number of Events in the ith Minimal Cut Set
S_k : The kth Term of the Inclusion–Exclusion
Q_t : Total Component Failure Frequency
α_k : Percentage for the Failure Frequency of k Components

References

[1]. K.N. Fleming, "A Reliability Model for Common Mode Failure in Redundant Safety Systems," Proceedings of the Sixth Annual Pittsburgh Conference on Modeling And Simulation, GA–A13284, General Atomic Company, April 1975.

[2]. J.A. Steverson and C.L. Atwood, "Common Cause Fault Rates for Valves," NUREG/CR–2770, Prepared for U.S. Nuclear Regulatory Commission by EG&G Idaho, Inc., February 1983.

[3]. C.L. Atwood, "Estimators for the Binomial Failure Rate Common Cause Model," NUREG/CR–1401, April 1980.

[4]. Pickard, Lowe and Garrick, Inc., *Seabrook Station Probabilistic Safety Assessment, Prepared for Public Service Company of New Hampshire and Yankee Atomic Electric Company, PLG–0300, December 1983.*

[5]. K.N. Fleming and A.M. Kalinowski, "An Extension of the Beta Factor Method to Systems with High Levels of Redundancy," Report PLG–0289, August 1983.

[6]. A.W. Marshall and I. Olkin, "A Multivariate Exponential Distribution," Journal of the American Statistics Association **62**, 30–44, 1967.

[7]. W.E. Vesely, "Estimating Common–Cause Failure Probability in Reliability and Risk Analysis : Marshall–Olkin Specialization," International Conference on Nuclear System Reliability Engineering and Risk Assessment, June 1977.

[8]. K.N. Fleming et al., "Classification and Analysis of Reactor Operating Experience Involving Dependent Events," EPRI NP-3967, Electric Power Research Institute, June 1985.

[9]. R.E. Barlow and F. Proschan, *Statistical Theory of Reliability and Life Testing-Probability Models,* Holt, Rinehart and Winston, Inc., 1975.

[10]. M.G.K. Evans, G.W. Parry and J. Wreathall, "On the Treatment of Common-Cause Failures in System Analysis," Reliability Engineering, **9**, 107-115, 1984.

[11]. *PRA Procedures Guide,* Nuclear Regulatory Commission, NUREG/CR-2300, 1983.

[12]. K.N. Fleming et al., "A Systematic Procedure for the Incorporation of Common Cause Events into Risk and Reliability Models," Nuclear Engineering and Design, **93**, 245-273, 1986.

[13]. R.R. Willie, "Computer Aided Fault Tree Analysis," Operations Research Center, University of California, Berkley, August 1978.

[14]. *Systems Manual-Pressurized Water Reactors,* Nuclear Regulatory Commission.

[15]. K.J. Yoo, et al., "Auxiliary Feedwater System Reliability Analysis of Nuclear Power Plants," Korea Electric Power Corporation, KRC-84N-T10, April 1985.