'2002 춘계학술발표회 논문집
한국원자력학회

위험도감시프로그램에서 공통원인고장 분석방법 연구

An Analysis on the Treatment of the Common Cause Failure in On-Line Risk Monitoring Program

김민철, 성게용, 이창주

한국원자력안전기술원
대전광역시 유성구 구성동 19

요 약

국내 규제기관에서는 원자력발전소에 대한 중대사고 정책을 발표하면서 2003년 이후 각 원전에 대해 위험도 감시계획을 수립·시행하도록 규정하고 있다. 이를 위해 공통원인고장의 정의를 이용하여 공통원인기기군 내의 특정기기가 고장 및 보수로 인해 이용불가능할 경우 다른 기기 및 계통이 어떠한 영향을 받는지를 살펴보았으며 이를 위험도 감시프로그램에서 정량적으로 평가할 수 있는 방법을 제안하였다.

Abstract

In Korea, the risk monitoring program will be developed of and applied to each plants till 2003 by the Severe Accident Management Plan. When a component among the common cause component group (CCCG) fails, other components in the CCCG may be affected and resulted in the failure probability increase. We proposed the methods of quantitatively evaluating the effects using the CCF definitions. These methods can be adopted to the risk monitoring program.

1. 서론

전세계적으로 규제기관 및 산업계에서는 확률론적안전성평가(Probabilistic Safety Assessment: PSA) 결과를 많은 분야에 이용하려 하고 있다. 그러한 이용은 결정론적인 평가방법에서 해석하기 어려운 분야에 한정되어져서 출발하였으나, 최근 그간의 경험 및 위험에 대한 각종 정보들을 종합하여 보다 원자력발전소를 안전하고 효율적으로 이용할 수 있는 방법에 적용하려 하고 있다.

이러한 전세계적인 추세에 발맞추어 국내에서는 중대사고 정책을 발표하면서, 원자력발전소의 안전성 확보 및 확인을 위해 실시간으로 발전소의 위험도를 평가하도록 규정하였다.

이러한 실시간 위험도 평가에 있어서, 발전소의 구성상태 변화를 어떻게 반영할 것인지 결정하는 것은 매우 중요한 요소이다. 본 논문에서는 가동중 발전소 구성상태 변화의 주 요인인 고장 및 보수로 인해 특정기기가 이용불가능할 경우에 증가되는 위험도를 어떻게 평가할 수 있는지에 대해 제안하였다.

2. 배경

공통원인고장(Common Cause Failure: CCF)의 발생이란 여러기기들의 동시고장, 즉 다중고장(Multiple Failures)을 의미하는 것으로, 특히 발전소의 안전성 확보를 위해 도입한 다중성(Redundancy)에 영향을 끼쳐 관련 계통의 기능상실로 인하여 원전 안전에 심각한 영향을 미칠 수 있다.

따라서 CCF에 대한 많은 연구가 수행되어 왔으며, WASH-1400[1]에서 처음으로 정량화 기법이 소개된 이래 최근에는 다음 기법들이 주로 이용되고 있다.: 1) Beta Factor 모델, 2) Multiple Greek Letter (MGL) 모델, 3) Alpha Factor 모델[2]. 이 세가지 방법은 기본모수모델(Basic Parameter Model)을 근간으로 하는 모델이다. 기본모수모델은 CCF 정량화시 이용되는 방법으로써 간단하게 설명한다면, 고장나는 기기의 개수에 초점을 두어 분석하는 방법이다.[2]

그림 1과 같이 A, B, C로 이루어진 간단한 계통을 예로 들어보았을 때, 기기 A, B, C의 고장사건은 아래와 같이 정의된다.

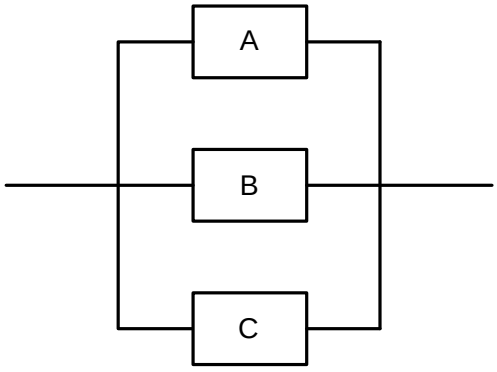

그림 1. 다중도가 3인 예제계통

$A_T = I_A + C_{AB} + C_{AC} + C_{ABC}$

$B_T = I_B + C_{AB} + C_{BC} + C_{ABC}$

$C_T = I_C + C_{AC} + C_{BC} + C_{ABC}$

여기에서 A_T, B_T, C_T는 기기 A, B, C의 모든 원인에 의한 고장사건, I_A, I_B, I_C는 각각의 독립고장사건, C_{AB}, C_{AC}, C_{ABC} 등은 공통원인 AB, AC, ABC에 의한 고장을 의미한다.

A_T, B_T, C_T에 대한 고장확률은 기본모수모델을 이용하여 다음과 같이 정량화할 수 있다.

$$Q_T = P[A_T] = P[I_A] + P[C_{AB}] + P[C_{AC}] + P[C_{ABC}]$$
$$= Q_1 + 2Q_2 + Q_3$$
$$= P[B_T] = P[C_T]$$

여기에서,

$P(I_A) = P(I_B) = P(I_C) = Q_1$

$P(C_{AB}) = P(C_{AC}) = P(C_{BC}) = Q_2$

$P(C_{ABC}) = Q_3$.

다중도(Redundancy)가 3인 그림 1과 같은 계통의 이용불능도 평가식은 최소단절집합(Minimal Cutsets: MCSs)을 이용하여 계산가능하다. 우선 최소단절집합은 다음과 같다: {($I_AI_BI_C$), (I_AC_{BC}), (I_BC_{AC}), (I_CC_{AB}), (C_{ABC})}. 계통이용불능도 Q_S는,

$$Q_S = \sum_{i=1}^{n} P(MCS_i) = Q_1^3 + 3Q_1Q_2 + Q_3$$

여기에서 n은 최소단절집합의 개수이다.

3. 공통원인고장 분석방법

3.1 기본개념

본 논문의 초점은 정상적으로 가동중이던 계통의 특정기기가 이용불능할 경우 이를 위험도 감시프로그램에 어떻게 반영할 것인가에 대한 것이다. 기기가 이용불능하게 되는 경우는 크게 두가지로 나누어질 수 있다: 1) 고장으로 인한 이용불능, 2) 보수로 인한 이용불능.

앞서 설명한 그림 1과 같은 간단한 계통을 다시 예로 들어, 만약 기기 C가 고장났을 경우 그 고장원인이 독립원인(I_C)인지 또는 공통원인(C_{AC}, C_{BC}, C_{ABC})인지는

알 수 없다. 기기 C의 고장원인이 독립원인이라면, 즉 다른 A, B 기기에 아무런 영향을 끼치지 않는다면 해당 계통에 더 이상의 특이한 사항이 발생하지 않는다. 그러나, 공통원인에 의해 발생한 고장이라면 동일한 원인에 의해 다른 기기가 영향을 받게 되고 추가 기기 작동시 기기 C의 고장과 동일하게 고장날 것이다.

따라서, 기기 C가 고장났을 경우 공통원인기기군(Common Cause Component Group: CCCG) 내에 속하는 다른 기기들은 영향을 받게 되고, 고장발생 확률은 증가하게 되며, 위험도 감시프로그램은 이러한 측면을 반영하여야만 한다.

그림 1과 같은 계통에서 보수로 인해 기기 C가 이용불능하게 될 경우는 앞선 경우와 다소 다르다. C의 이용불능은 다른 기기에 영향을 끼치지 않고 다만 계통에 영향을 끼치게 되는데, 계통의 성공기준이 1-out-of-3에서 1-out-of-2로 바뀌게 된다.

따라서 기기 C가 보수 또는 테스트로 인해 이용불능하게 될 경우 공통원인기기군 내에 속하는 다른 기기들은 영향을 받지는 않으나 계통의 성공기준이 바뀌게 됨에 따라 위험도 감시프로그램은 이러한 측면을 반영하여야만 한다.

보다 자세한 평가방법은 아래 절에서 다루도록 하겠다.

3.2 고장으로 인한 기기 이용불능시

그림 1과 같은 계통에서, 만약 기기 C가 고장났다면 계통과 기기는 다음과 같은 영향을 받게 된다.

1) 계통 : 성공기준의 변화

2) 기기 : 고장확률의 증가

우선, 기기 C의 고장을 PSA에서 정의하고 있는 기본사건(Basic Event)에 따라 구분하면 다음 네가지 중 하나에 속한다: 1) 기기 C의 독립고장(I_C), 2) 기기 A와 C의 CCF(C_{AC}), 3) 기기 B와 C의 CCF(C_{BC}), 4) 기기 A, B, C의 CCF(C_{ABC}).

즉, 공통원인기기군 내의 다른 기기들의 상태를 확인하기 전까지 기기 C의 고장은 위의 네가지 형태중에 하나가 될 것이고, 각각의 조건부확률은 다음과 같다.[3]

$$P[I_C \mid C \text{ failed}] = \frac{P[(I_C) \cap (C \text{ failed})]}{P[C \text{ failed}]} = \frac{P[I_C]}{P[C \text{ failed}]} = \frac{Q_1}{Q_T} = 1-\beta$$

$$P[C_{AC} \mid C \text{ failed}] = \frac{P[(C_{AC}) \cap (C \text{ failed})]}{P[C \text{ failed}]} = \frac{P[C_{AC}]}{P[C \text{ failed}]} = \frac{Q_2}{Q_T}$$
$$= \beta(1-\gamma)/2$$

$$P[C_{BC} \mid C \text{ failed}] = \frac{P[(C_{BC}) \cap (C \text{ failed})]}{P[C \text{ failed}]} = \frac{P[C_{BC}]}{P[C \text{ failed}]} = \frac{Q_2}{Q_T}$$
$$= \beta(1-\gamma)/2$$

$$P[C_{ABC} \mid C \text{ failed}] = \frac{P[(C_{ABC}) \cap (C \text{ failed})]}{P[C \text{ failed}]} = \frac{P[C_{ABC}]}{P[C \text{ failed}]} = \frac{Q_3}{Q_T}$$
$$= \beta\gamma$$

여기에서 β와 γ는 MGL 모델의 모수를 나타낸다.

즉, 기기 C가 고장났을 때, 그 고장의 형태가 독립고장일 확률은 (1-β), 기기 A, C 또는 기기 B, C의 공통원인고장일 확률은 β(1-γ)/2 이며 기기 A, B, C의 공통원인고장일 확률은 (βγ) 가 됨을 알 수 있다.

기기 C의 고장이 위 네가지 형태로 구분되어질 때 기기 A와 B는 다음과 같이 영향을 받게 된다.

첫 번째, 기기 C의 고장이 독립고장일 경우, 기기 A와 B는 아무런 영향이 없다. 두 번째, 기기 C의 고장이 C_{AC}일 경우, 기기 A는 동일한 원인과 연계요인에 의해 고장날 것이고 기기 B는 아무런 영향이 없을 것이다. 세 번째, 기기 C의 고장이 C_{BC}일 경우, 기기 A는 아무런 영향이 없고 기기 B는 같은 원인과 연계요인이 의해 고장날 것이다. 마지막으로, 기기 C의 고장이 C_{ABC}일 경우, 기기 A와 B는 C와 마찬가지로 고장날 것이다. 이러한 분석은 아래와 같이 정량화 되어질 수 있다.

ⅰ) 기기 C의 고장이 독립고장일 경우, $P[A_T] = Q_T$, $P[B_T] = Q_T$

ⅱ) 기기 C의 고장이 C_{AC}일 경우, $P[A_T] = 1$, $P[B_T] = Q_T$

ⅲ) 기기 C의 고장이 C_{BC}일 경우, $P[A_T] = Q_T$, $P[B_T] = 1$

ⅳ) 기기 C의 고장이 C_{ABC}일 경우, $P[A_T] = 1$, $P[B_T] = 1$

따라서 기기 C가 고장났을 경우, A가 고장날 확률 Q_T^*는

$$Q_T^* = Q_T\frac{Q_1}{Q_T} + (1)\frac{Q_2}{Q_T} + Q_T\frac{Q_2}{Q_T} + (1)\frac{Q_3}{Q_T} \qquad \text{식 (1)}$$
$$= Q_1 + Q_2\left(1 + \frac{1}{Q_T}\right) + \frac{Q_3}{Q_T}$$

와 같이 된다.

기기 C와 관계된 기본사건의 발생확률은 $1/Q_T$ 만큼 증가함을 알 수 있다. 표 1에 각각의 기본사건에 대한 기기 C의 고장발생 전·후의 기본사건 발생확률을 정

리하여 나타내었다.

표 1. 기기 C의 고장발생 전·후의 기본사건 발생확률 변화

구분	I_A	I_B	I_C	C_{AB}	C_{BC}	C_{AC}	C_{ABC}
전	Q_1	Q_1	Q_1	Q_2	Q_2	Q_2	Q_3
후	Q_1	Q_1	Q_1/Q_T	Q_2	Q_2/Q_T	Q_2/Q_T	Q_3/Q_T

위험도 감시프로그램의 해당 기본사건 발생확률을 변경하여 기기 C의 고장에 따라 증가된 위험도를 고려할 수 있다.

그러나, 앞서 설명하였던 것처럼 계통 측면에서 보았을 때, 기기 C의 고장에 따라 계통의 성공기준이 변화하게 된다. 또한 실제 위험도 감시프로그램에 사용될 수 있는 고장수목(Fault Tree)를 보면, 보수로 인한 이용불능을 기본사건으로 고려하고 있어서 단순하게 발생확률만을 변경하여서는 안되는 경우가 발생할 수 있다. 하지만, 보통의 경우 기기 보수로 인한 이용불능도가 전체 계통이용불능도에 기여하는 정도는 무시할 정도로 작다.

기기 C가 고장났을 때, 고장수목에 모델링 하는 방법은 다음과 같이 크게 두 가지로 나누어 볼 수 있다.

1) 고장난 기기 C가 없다고 가정하여 모델링하는 방법
2) 고장난 기기 C가 있다고 가정하여 모델링하는 방법

첫 번째, 고장난 기기 C가 없다고 가정하여 모델링하는 경우에는 계통의 성공기준이 변경되고, 그에 따라 기본사건 발생확률을 어떻게 정의할 것인가와 같은 문제가 발생한다.

위에서 고려한 기본사건들은 각각 동시에 발생할 수 없는 상호배반사건(Mutually Exclusive Event)으로 가정하고 있다. 즉, C_{AB}와 C_{ABC}는 동시에 발생할 수 없다. 이러한 공통원인고장 분석시의 가정을 근거로 하여 계통 성공기준의 변화에 따른 기본사건 발생확률을 정의하도록 하겠다.

식(1)은 다중도가 3인 그림 1과 같은 계통에서 한 개의 기기가 고장났을 때 해당 공통원인기기군 내의 다른 기기의 고장이 발생할 확률을 계산하는 식이다. 정성적으로 분석하더라도 기기 A의 독립원인고장(I_A)은 기기 C의 고장에 아무런 영향을 받지 않는다. 앞서 설명한 것처럼 각각의 기본사건들은 상호배반사건이기 때문이다. 이는 기기 B의 독립원인고장에도 동일하게 적용된다. 공통원인고장 중에서 기기 A

와 B가 동시에 고장나는 사건의 경우 역시 위와 마찬가지의 이유로 기기 C의 고장에 아무런 영향을 받지 않는다.

그러나, 기기 A, C(C_{AC}), 기기 B, C(C_{BC}) 그리고 기기 A, B, C(C_{ABC})의 공통원인고장과 같이 기기 C가 포함된 기본사건의 경우는 앞서 설명한 바와 같이 기기 C의 고장에 영향을 받게되고, 각각의 기본사건 발생확률은 $1/Q_T$배 만큼 증가하게 되고 계통의 이용불능도 역시 증가하게 된다.

따라서 고장난 기기 C가 없다고 가정하여 모델링할 경우 고장수목도에서 기기 C와 관계된 트레인을 단순하게 삭제하여 계산하여서는 안된다.

예를 들어, 그림 1과 같은 계통에 대하여 보수로 인한 이용불능을 고려한 고장수목을 작성하여 그림 2에 나타내었다. 기기 A, B, C 각각에 대한 요구시 고장확률을 0.004/D(=Q_T), 보수로 인한 이용불능도를 1.76×10^{-3}(=M_A=M_B=M_C=Q_M), 그리고 MGL 모수인 β를 0.074, γ는 0.689라 가정하였고, 2개 이상의 기기를 동시에 보수할 수 없다고 가정하였다.

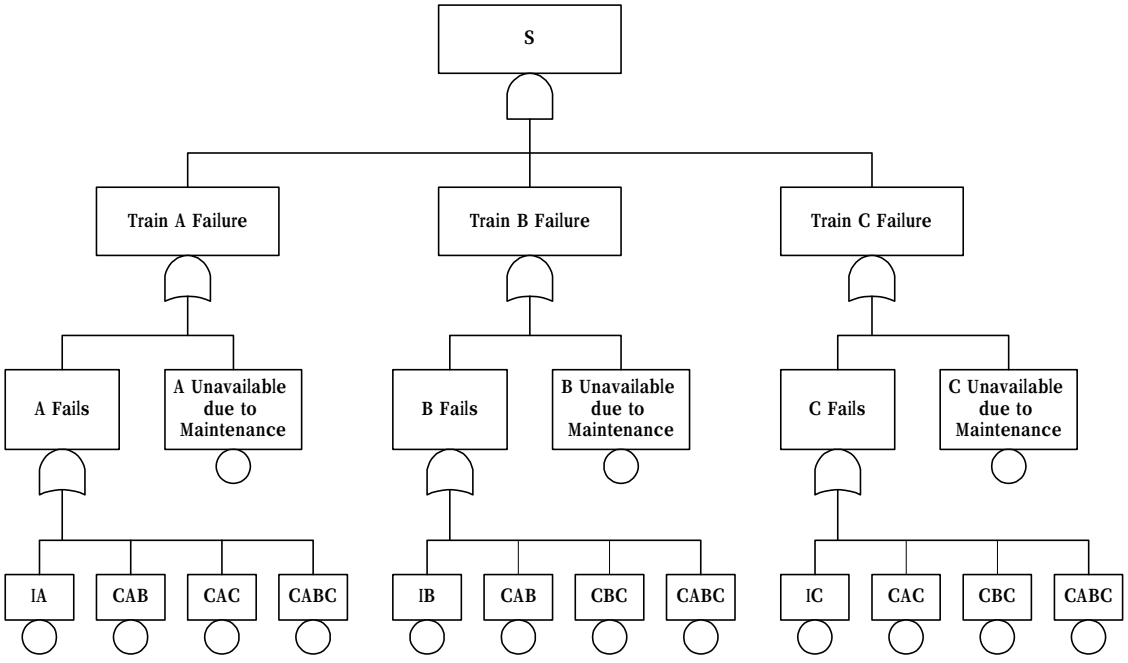

그림 2. 예제계통(다중도=3)에 대한 고장수목도

이러한 가정에서 기본모수 Q_1, Q_2, Q_3를 계산하면 다음과 같다: 1) Q_1 = 3.704×10^{-3}, 2) Q_2 = 4.603×10^{-5}, 3) Q_3 = 2.039×10^{-4}. 그리고 계통의 이용불능도(Q_S)는,

$Q_S = Q_1^3 + 3Q_1Q_2 + Q_3 + 3Q_M(Q_1^2+Q_2) = 2.048\times10^{-4}$

이 된다.

위에서 살펴본 바와 같이 기기 C가 고장났을 때의 기본사건 발생확률은

$I_A(Q_1)$	$I_B(Q_1)$	$I_C(Q_1^*)$	$C_{AB}(Q_2)$	$C_{BC}(Q_2^*)$	$C_{AC}(Q_2^*)$	$C_{ABC}(Q_3^*)$
3.704×10^{-3}	3.704×10^{-3}	9.26×10^{-1}	4.603×10^{-5}	1.151×10^{-2}	1.151×10^{-2}	5.098×10^{-2}

과 같으며, 이 값들을 이용하여 계통이용불능도를 계산하면,

$Q_S^* = Q_1^2Q_1^* + Q_1(Q_2+2Q_2^*) + Q_3^* + Q_M(Q_1^2+2Q_1Q_1^*+Q_2+2Q_2^*) = 5.113\times10^{-2}$

가 된다.

또한 기기 C가 없다고 가정하여 계산해보면,

$Q_{S\ No\ C} = Q_1^2 + Q_2 = 4.617\times10^{-3}$

이 된다.

Q_S, Q_S^*, 그리고 $Q_{S\ No\ C}$ 값을 비교하였을 때, Q_S^*와 $Q_{S\ No\ C}$ 둘 모두 기기 C가 고장나기 전보다 위험도를 높게 계산하고 있으나, $Q_{S\ No\ C}$ 는 Q_S^*에 비해 10배 정도 낮게 계산하고 있다. 즉, 단순하게 기기 C가 없는 상태에서 계산한다면 실제의 위험도에 비해 낮게 평가할 수 있음을 알 수 있다.

다시 말해, 기기 C가 없다고 가정하여 평가할 경우에는 기기 C의 고장에 대한 공통원인기기군 내의 다른 기기들의 고장발생확률을 재평가하여 전체계통의 이용불능도를 평가하여야 한다.

다중도가 3인 예제 계통을 다시 살펴보면, 기기 C가 없기 때문에, 기본사건 C_{AC}, C_{BC}, C_{ABC}는 삭제되고 C_{AB}와 I_A, I_B 만 남게 된다. 앞서 설명한 바와 같이 기기 A와 B의 독립고장은 기기 C 고장에 영향을 받지 않는다. 근본원인과 연계요인을 고려해보면 문제해결이 다소 복잡해진다. 예를 들어, C_{AC}의 경우 기기 C가 없기 때문에 A와 C간의 연계요인은 없어졌다. 하지만 기기 A와 C의 고장을 동시에 유발시키는 원인은 여전히 이용가능한 기기 A에 영향을 끼치게 되고 고장을 유발시킬 수 있다. 따라서 C_{AC}의 발생확률은 I_A에, C_{BC}의 발생확률은 I_B, C_{ABC}의 발생확률은 C_{AB}에 포함되어 다음과 같이 계산되어야 한다.

$$Q_1^* = Q_1 + Q_2^* = Q_1 + \frac{Q_2}{Q_T}$$

$$Q_2^* = Q_2 + Q_3^* = Q_2 + \frac{Q_3}{Q_T}$$

가 된다.

두 번째, 고장난 기기 C가 있다고 가정하여 모델링하는 경우에는 이용 불가능한 기기 C를 가동 가능한 것으로 가정하였기 때문에 발생가능한 문제들을 어떻게 해결할 것인가 하는 문제가 있다.

이와 같은 방법에 따라 평가할 경우는 위의 Q_S^*와 같이 계산되어진다. 조금 더 자세하게 살펴보면, 기기 C의 고장과 보수로 인한 기기이용불능도를 동시에 고려하고 있기 때문에 전체적으로 기기 C에 대한 이용불능도가 1보다 커지게 된다. 하지만 보수로 인한 기기 이용불능도가 계통이용불능도에 기여하는 정도가 미미하기 때문에 평가자체에는 크게 영향을 끼치지 않는다. 따라서 정량적 평가 자체에만 목적을 둔다면 사용가능한 방법으로 볼 수 있으나 계통의 변화를 제대로 모사하지 못하고 있다는 측면과 생성되어서는 안되는 최소단절집합으로 인해 중요도 분석 등 결과활용 측면에 문제가 있을 수 있다.

3.3 보수에 따른 기기 이용불능시

앞선 절에서 보았던 것과 마찬가지로 그림 1과 같은 다중도가 3인 계통에서, 만약 기기 C가 보수로 인해 이용불가능하게 된다면, 계통의 성공기준이 1-out-of-3에서 1-out-of-2로 변하게 됨을 쉽게 알 수 있다.

공통원인고장의 분석방법인 근본원인과 연계요인을 고려하여 자세하게 살펴보면, 앞서 설명한 것과 동일하다. 기기 A, C의 공통원인고장의 연계요인은 없어졌으나 기기 A의 고장을 유발하는 원인은 A가 가동하는 한 여전히 남아있게 된다. 따라서 보수로 인해 특정기기가 이용불가능할 경우, 해당 공통원인기기군 내의 다른 기기들은 직접적인 영향을 받지는 않으나 공통원인고장의 정의에 따라 고장율은 다소 다음과 같이 다소 증가하게 된다.

$$Q_{1M}^* = Q_1 + Q_2$$

$$Q_{2M}^* = Q_2 + Q_3$$

4. 결론

국내 규제기관에서는 원전의 중대사고 정책을 발표하여 2003년부터 각 원전에 대해 위

험도 감시계획을 수립하여 시행하도록 하고 있다. 위험도 감시를 감시하기 위해서는 실시간 위험도 감시프로그램을 개발·설치·시행하여야만 하는데, 이러한 위험도 감시에 있어서 수시로 발생할 수 있는 경우인 공통원인기기군 내의 특정기기가 고장 또는 보수로 인해 이용불가능할 경우 실시간 위험도 감시프로그램에서 이를 어떻게 반영하여야 하는지에 대하여 논하였다. 본 논문에서는 공통원인고장 발생 매카니즘 분석 방법인 근본원인과 연계요인 등을 이용하여 평가방법을 제안하였다.

참고문헌

[1] U.S. Nuclear Regualtory Commission, Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400, NUREG-75-014, 1975.

[2] A. Mosleh, K. N. Fleming, G. W. Parry, H. M. Paula, D. H. Worledge and D. M. Rasmuson, Procedures for Treating Common Cause Failures in Safety and Reliability Studies, Vol 1 & 2, NUREG/CR-4780, EPRI NP-5613, 1988.

[3] Zdenko Simic, et. al., On-line Operation Support Modeling: Common Cause Dependency, PSA '99, 1999.

[4] KEPCO, Final Probabilistic Safety Assessment Report for Ulchin units 3&4, 1998.