IE Interfaces
Vol. 25, No. 4, pp. 382-392, December 2012. http://dx.doi.org/10.7232/IEIF.2012.25.4.382
ISSN 1225-0996 | EISSN 2234-6465 | © 2012 KIIE

디지털 원자로 보호시스템의 공통원인고장 분석에 관한 사례연구

공명복[1†] · 이상용[2]

[1]울산대학교 산업경영공학부 / [2]포뉴텍 R&D 센터

A Case Study of the Commom Cause Failure Analysis of Digital Reactor Protection System

Myung-Bock Kong[1] · Sang-Yong Lee[2]

[1]School of Industrial Engineering, University of Ulsan, Ulsan, 680-749
[2]R&D Center, Ponutech, Ulsan, 680-801

Reactor protection system to keep nuclear safety and operational economy of plants requires high reliability. Such a high reliability of the system can be achieved through the redundant design of components. However, common cause failures of components reduce the benefits of redundant design. Thus, the common cause failure analysis, to accurately calculate the reliability of the reactor protection system, is carried out using alpha-factor model. Analysis results to 24 operating months are that 1) the system reliability satisfies the reliability goal of EPRI-URD and 2) the common cause failure contributes 90% of the system unreliability. The uncertainty analysis using alpha factor parameters of 0.05 and 0.95 quantile values shows significantly large difference in the system unreliability.

Keyword: reactor protection system, redundant design, common cause failure, alpha factor model, (un)reliability, uncertainty

1. 서 론

원자력 발전소의 원자로 보호시스템은 원자로 정지시스템과 공학적 안전설비 작동시스템을 제어하기 위한 설비이다. 원자로 운전에 대한 모든 정보는 항상 원자로 보호시스템에 입력신호로 전달된다. 만약 입력신호가 보호시스템에 설정된 값을 초과하면 보호시스템은 원자로를 정지시키기 위하여 제어봉에 가해지는 전원을 차단하여 제어봉을 떨어뜨리도록 하는 신호와 혹시 발생할지도 모를 방사능 누출 사고의 확산을 방지하기 위하여 안전설비를 작동시키는 신호를 출력한다. 따라서 원자로에 이상이 있을 때 보호시스템이 고장으로 제 기능을 하지 못하면 발전소의 안전을 위협하는 중대한 사고를 야기하게 된다. 또한 원자로에 이상이 없을 때 보호시스템에 고장이 발생하면 최악의 상태에 대비하기 위하여 정상인 원자로를 정지시켜야하므로 발전소의 가동률을 떨어뜨려 경제적 손실을 발생시킨다. 즉 원자로 보호시스템은 높은 신뢰성이 요구된다.

원자로 보호시스템은 신뢰성이 높아야 할 뿐만 아니라 최근에 전자장비의 디지털화 경향에 따라 디지털화된 장비로 바뀌고 있으나 디지털화된 장비의 예측되지 않은 고장을 방지하기 위하여 4중화 채널구조를 다시 이중화하여 많은 중복 구성품을 가진 복잡한 설계를 채택하고 있다.

중복설계는 시스템의 신뢰성을 높이는데 중요한 역할을 한

이 논문은 울산대학교 교내 연구비(2011-0151) 지원으로 연구되었음.
†연락저자 : 공명복 교수, 680-749 울산광역시 남구 대학로 93 울산대학교 산업경영공학부,
Fax : 052-259-1683, E-mail : mbkong@ulsan.ac.kr
투고일(2012년 07월 30일), 심사일(1차 : 2012년 09월 05일, 2차 : 2012년 10월 15일), 게재확정일(2012년 10월 15일).

다(Shooman, 2002). 그러나 2개 이상의 구성품이 하나의 원인으로 동시에 고장나는 공통원인고장은 독립적인 중복설계의 이점을 감소시킨다. 공통원인고장에 대한 분석은 시스템 설계에서 구성품들의 공통원인고장에 대한 취약성을 발견하고 이로부터 야기되는 시스템의 고장위험을 줄이기 위한 것이다(Ericson, 2005). 분석을 위하여 공통원인고장을 시스템에 고려하는 2가지 방법이 있다(Fleming and Mosleh, 1985). 명시적 방법(Explicit Method)과 묵시적 방법(Implicit Method)이 그것이다. 명시적 방법은 공통원인고장 사건을 공통원인부품 그룹에 속하는 부품의 고장에 반복되는 기본사건으로서 시스템의 결함나무나 신뢰성블록그림에 추가하는 방법이다. 그 후 전통적인 결함나무분석이나 신뢰성블록그림분석을 통하여 최소 컷집합(Minimal Cut Set)이나 최소 패스집합(Minimal Path Set)을 구하고 기본사건의 확률을 사용하여 정량적 분석을 행하는 것이다. 반면에 묵시적 방법은 공통원인고장을 고려하지 않고 결함나무나 신뢰성블록그림을 작성하여 시스템의 대수적 불신뢰도 표현식을 구하고 그 표현식에 공통원인고장 사건을 포함시키는 것이다. 정량적 분석은 공통원인고장이 포함된 표현식에 사건의 발생확률을 치환하여 하게 된다. 그러나 이들 모두 규모가 큰 결함나무모형에 적용하기가 용이하지 않다. 명시적 방법은 공통원인사건을 추가한 확장된 결함나무나 신뢰성블록그림을 작성해야 하기 때문이고 묵시적 방법은 확장된 결함나무나 신뢰성블록그림을 작성할 필요가 없어 편리하지만 공통원인고장사건이 포함된 시스템에 대한 대수적 표현을 구하는 것이 용이하지 않기 때문이다. 따라서 대수적 표현을 쉽게 얻기 위하여 이항의사결정그림을 사용하는 방법이 제시되기도 하였다(Tang and Dugan, 2004).

Kong and Lee(2010)는 독립고장의 발생만을 고려하여 원자로 보호시스템의 안전성을 평가하였다. 본 논문은 동일한 원자로 보호시스템에 대하여 중복설계의 효과에 대한 정확한 평가를 위하여 공통원인고장에 대하여 분석하고자 한다. 분석방법은 묵시적 방법에서와 같이 공통원인고장을 고려하지 않은 결함나무를 작성하여 최소 컷집합을 구한 후 선별된 공통원인고장그룹을 고려하여 최소 컷집합을 확장하여 발생가능한 공통원인고장 최소 컷집합을 작성한다. 다음으로 공통원인고장을 모형화하는 모수모형(Mosleh *et al*., 1988) 중에서 알파인자모형을 적용하여 정량적 분석을 행한다. 이와 같이 하는 이유는 공통원인고장에 대하여 정성적 및 정량적 평가를 함께 하기 위한 것이다.

Eide *et al*.(1999)은 명시적 방법을 사용하고 공통원인고장에 알파인자모형을 적용하여 4영역으로 분할된 원자로 정지시스템의 불신뢰도를 계산하였다. Kamyab *et al*.(2010)은 명시적 방법에 다중 그리스문자 모형을 사용한 공통원인고장을 고려하여 원자로 노심냉각시스템의 신뢰도를 분석하였다.

본 논문의 구성은 제 2장에서는 디지털 원자로 보호시스템에 대한 기능과 구조, 구성모듈에 대하여 설명하고, 제 3장에서는 공통원인고장 분석절차에 따라 선별분석 및 상세한 정량적분석을 행하고 시스템의 불신뢰도에 대하여 밝혀진 사실에 대하여 기술할 것이다. 제 4장은 결론이다.

2. 디지털 원자로 보호시스템

디지털 원자로 보호시스템은 독립된 4개의 채널로 구성된다. 또한 각 채널은 이중화되어 있어 각 채널의 구성품인 모듈은 2개씩이다. 각 채널은 바이스테이블 모듈(BSM), 동시논리 모듈(CCM), 원자로정지 개시모듈(RIM), 공학적 안전설비 개시모듈(EIM)로 구성된다. <Figure 1>은 디지털 원자로 보호시스템의 구조를 나타내는 블록도이다.

BSM은 노심보호시스템과 안전등급계측 시스템으로부터 계측신호를 입력받는다. 모듈의 주요한 기능은 입력된 계측신호를 설정값와 비교하여 트립이나 예비트립 신호를 출력한다. 또한 원자로의 기동과 정지 시에 불필요한 트립을 막기 위해 운전우회 기능도 가진다. 운전우회는 각 채널에서 안전 변수값이 기 설정된 범위 내에 있을 때 운전원에 의해 수동으로 입력되고 설정 범위를 벗어나면 자동으로 제거된다. 그 밖에 제어봉 집합체 인출금지 신호를 출력제어 시스템으로 보내기도 한다.

CCM은 BSM으로부터 트립신호를 입력 받는다. 하나의 BSM의 신호는 다른 3개의 채널의 CCM에도 입력으로 제공된다. 각 채널의 CCM은 각각의 BSM의 트립신호에 대한 동시논리 알고리즘을 수행한다. 동시논리 알고리즘은 트립된 채널과 우회된 채널의 신호 상태를 기반으로 동시논리 출력의 상태를 결정하는 것이다. 채널우회는 출력운전 상태에서 트립된 채널의 보수 및 시험을 할 수 있도록 제어실과 보수시험반에서 수동으로 개시된다. CCM의 동시논리 출력은 4개 채널 중 최소한 2개 채널이 트립된 상태일 때 출력신호를 생성한다. 즉 하나의 채널 우회 시 2/3 동시논리로, 두 채널 우회 시 2/2 동시논리로 트립신호를 생성한다. 이와 같은 동시논리의 사용은 신호 자체의 신뢰성을 높이기 위한 것이다.

RIM은 CCM으로부터 최종 트립 출력을 받으며 2개 트레인의 신호를 병렬로 하여 각 채널의 신호에 대해 2/4 작동논리로 원자로 정지시스템을 구동시킨다. 마찬가지로 EIM도 같은 원리로 공학적 안전설비 작동시스템을 구동시킨다. 원자로 정지시스템과 공학적 안전설비 작동시스템은 동시적으로 구동되어야 하므로 신뢰성 구조상으로 표현하면 직렬구조이다. <Figure 1>은 원자로 보호시스템을 구조로 4종류의 모듈들이 배치되어 있는 4개의 채널과 각 채널에 대하여 A, B로 표시된 2개의 트레인을 보여주고 있다. 채널들은 스위칭설비에 의해 서로 통신네트워크를 이루며 또한 동일 트레인끼리 연결되어 정보를 공유한다.

3. 원자로 보호시스템의 공통원인고장 분석

원자력 발전소의 운전에는 핵과 관련한 안전성과 전력생산의

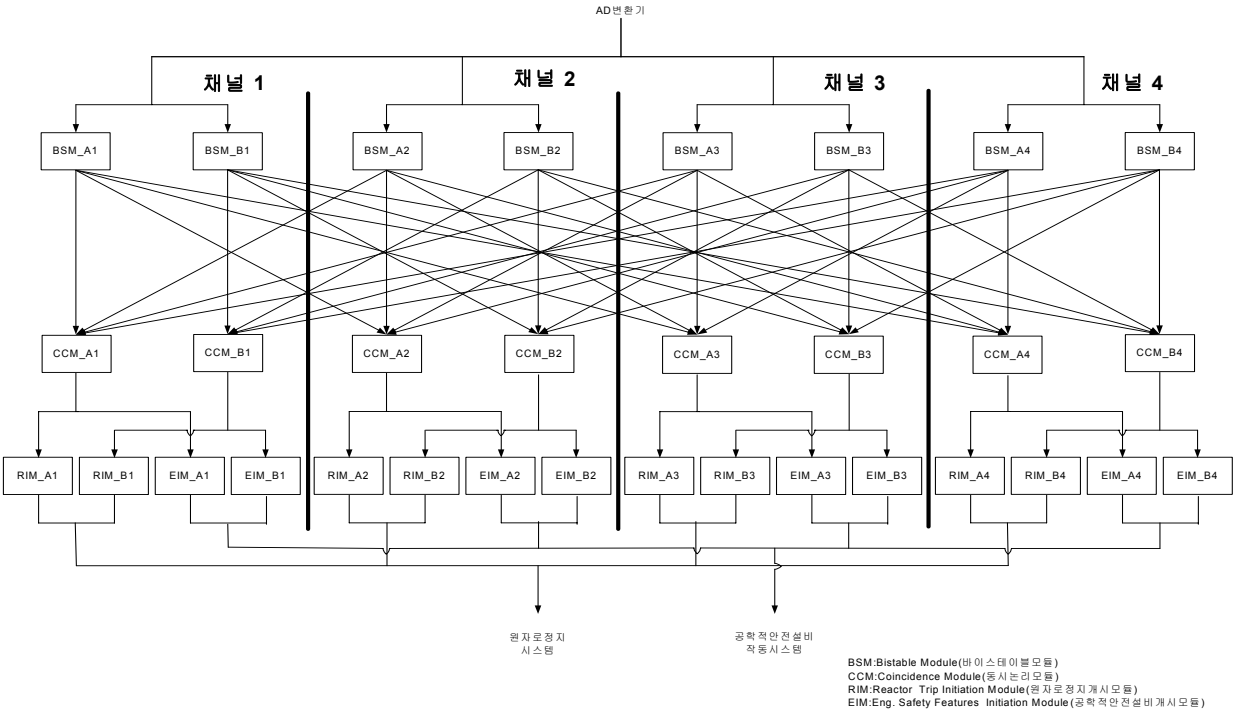

Figure 1. 디지털 원자로 보호시스템의 블록도

경제성을 동시에 고려해야 한다. 따라서 발전소의 원자로 보호시스템은 신뢰도와 가용도를 높이기 위하여 중복설계를 사용하고 있다. 따라서 <Figure 1>과 같이 4종류의 모듈을 8개씩 사용하여 4개 채널과 2개의 트레인으로 구성되어 있다. CCM은 2개 채널까지 우회가능한 다수결 논리 구조를 가지고 있으며 RIM과 EIM의 출력신호는 4 중 2 논리구조로 원자로 정지시스템과 공학적 안전설비 작동시스템에 입력되는 복잡한 신뢰도 구조를 가지고 있다.

공통원인고장(Common Cause Failure : CCF)은 독립적으로 구성한 중복설계의 이점을 파괴하는 단일고장이다. CCF 분석은 중복설계를 채택한 시스템에서 CCF를 일으키는 설계 취약성을 발견하고 평가하여 위험을 감소시키기 위한 재설계에 도움을 준다. 따라서 본 절에서는 원자로 보호시스템의 중복설계에 대한 CCF 분석을 행하고자 한다.

Mosleh *et al.*(1998)은 CCF 분석에 대하여 선별분석, 상세한 정성적 분석, 상세한 정량적 분석의 3단계 절차를 제시하고 있다. 선별분석은 분석하고자하는 시스템을 정의하고 결함나무를 작성한 후 CCF에 대한 취약성을 사전적으로 분석하는 것이다. 이 단계에서는 보수적인 관점에서 주어진 CCF에 민감할 것으로 생각되는 모든 구성품의 목록을 작성한다. 효율적인 선별의 실행방법은 연계인자(Coupling Factor)에 초점을 맞추는 것이다. 이와 같이 해서 작성된 부품들의 그룹을 공통원인부품그룹(Common Cause Component Group : CCCG)이라 한다. 이들은 CCCG의 모든 부품이 고장을 일으키는 전역 공통원인고장사건을 추가한 결함나무의 정량적 분석을 통하여 시스템의 불신뢰도에 영향이 적은 CCCG를 제거하고 영향이 큰 중요한 CCCG만을 선택하게 된다. 상세한 정성적 분석은 선별분석을 통하여 얻어진 CCCG를 시스템이 사용되는 발전소의 상황에 맞게 고려하고 시스템의 신뢰도 개선에 관한 공학적 의사결정도 얻기 위한 과정이다. 여기에는 운전경험의 검토, 발전소 설계와 운전방법의 검토, 근본원인과 연계인자에 대한 방어수단의 개발이 주된 업무이다. 상세한 정량적 분석은 공통원인기본사건(Common Cause Basic Event)을 확인하여 결함나무에 병합하고 CCF 모형을 적용하여 결함나무분석을 통해 시스템의 불신뢰도를 구하는 것이다. CCF 모형의 모수로는 CCF와 관련한 일반적 추정값이나 이것에 과거의 운전데이터를 고려한 베이지안 추정값이 보통 사용된다.

일반적으로 CCF 분석은 기술한 것과 같이 3단계로 진행되지만 새롭게 설계되는 시스템의 경우는 운전경험이 없으므로 2단계의 상세한 정성적 분석을 생략하고 선별분석 후 바로 상세한 정량적 분석으로 넘어갈 수 있다. 새로이 설계되고 있는 디지털 원자로 보호시스템에 대하여 상세한 정성적 분석을 생략하고 선별분석 후 상세한 정량적 분석을 행하다.

3.1 선별분석

원자로 보호시스템의 CCF에 대한 민감성을 확인하기 위하여 우선 CCF를 방어하는 방법과 무관하게 시스템을 구성하는 모듈 간에 연계인자를 확인한다. 연계인자는 CCF를 다중 독립고장과 구별되게 하는 것으로 2개 이상의 구성품에서 발생한 고장이 고장원인과 고장메카니즘 모두에서 유사한 특성을 보일 때 존재하는 것이다. 원자로 보호시스템은 BSM, CCM, RIM,

EIM으로 구성되어 있고 모든 모듈은 DSP, NIC 카드를 가지고 있으며 RIM의 경우는 DO 카드를 더 가지고 있다. Kong and Lee(2010)는 내결함성(Fault Tolerance)을 가지는 DSP 카드의 고장을 근사적으로 지수분포화 하는 것에 대한 근거를 제시하고 고장률을 구하였으며 여기에 다른 구성카드의 고장률을 합하여 모듈의 고장률을 <Table 1>과 같이 산출하였다.

Table 1. 모듈의 구성카드와 시간당 고장률

모듈	BSM	CCM	RIM	EIM
구성카드	DSP, NIC	DSP, NIC	DSP, NIC, DO	DSP, NIC
고장률(h-1)	5.92207×10^{-6}	5.92207×10^{-6}	9.58714×10^{-6}	5.92207×10^{-6}

CCCG를 분류해 내기 위하여 각 모듈에 대하여 연계인자로 동일한 설계, 동일한 하드웨어, 동일한 기능, 동일한 설치-정비-운전요원, 동일한 시험 절차, 동일한 인터페이스, 동일한 위치, 동일한 환경 등을 고려해 본다. 4종류의 모듈들은 동일하게 설계되었으며 동일한 DSP나 NIC 카드를 공통으로 가지고 있고 또한 설치-정비-운전요원이 동일하므로 모두 하나의 CCCG로 분류될 충분한 개연성을 가지고 있다. 그러나 기능, 인터페이스, 위치 및 환경 등에서 차이가 존재하여 모든 모듈들을 하나의 CCCG로 분류하지 않는다.

특히 디지털 시스템의 특성상 이종 모듈간의 CCF에 대한 연계인자로 통신 네트워크를 평가해야 한다. 따라서 이종 모듈간의 네트워크에서 접점기기의 주기적 중복체크(Cyclic Redundancy Check) 등을 포함한 방어기능을 검토한 결과 한 종류의 모듈의 촉발사건이 다른 종류의 모듈로 확산되는 것을 방지하기에 충분함이 파악되어 이종 모듈은 하나의 CCCG로 묶지 않았다. 동종 모듈간의 CCF에 대한 연계인자는 모듈들이 하나의 캐비넷에서 동일한 위치에서 동일한 기능을 수행하도록 되어 있고 또한 정성적 결함나무분석에서 같은 형태의 최소 컷집합에 포함되어 있으므로 동종 모듈들은 하나의 CCCG으로 분류한다. 따라서 채널과 트레인에 관계없이 8개의 BSM, 8개의 CCM, 8개의 RIM, 8개의 EIM을 각각의 CCCG로 하여 4개의 CCCG가 구성된다.

한편 4개의 CCCG 중에서 원자로 보호시스템의 불신뢰도에 영향이 적은 CCCG가 존재하는지 살펴보기 위하여 전역 공통원인고장사건이 추가된 결함나무를 작성하여 분석한다. 전역 공통원인고장사건은 각 CCCG 내의 모든 모듈이 고장을 일으키는 기본사건으로 고장률 λ_g는 식 (1)과 같은 베타인자 모형이 사용된다. 한편 각 모듈의 독립고장에 대한 고장률 λ_I는 식 (2)로 주어진다.

$$\lambda_g = g\,\lambda_T \tag{1}$$

$$\lambda_I = (1-g)\,\lambda_T \tag{2}$$

여기서 λ_T는 하나의 모듈에 대한 총고장률이다.

종속인 n중 k 정상($k \le n \le 4$) 시스템에 대하여 전역 공통원인인자 g의 값이 주어져 있다(Mosleh *et al.*, 1998). 한편 분석하고자 하는 원자로 보호시스템에 대하여 동종 모듈의 최소 컷집합(<Table 2>참조)이 6개의 모듈로 구성되어 있어, 반대로 각 CCCG의 모듈 8개 중에서 3개 이상의 모듈이 정상이면 시스템이 정상이므로 8 중 3 정상 시스템으로 간주한다. 시스템의 구성품이 동시에 시험되는 비순차시험(Non-Staggered Test)이냐 아니면 정해진 시간 간격으로 한 번에 하나씩 시험되는 순차시험(Staggered Test)이냐에 따라 다른 g값이 적용된다. 8 중 3 정상 시스템에서 순차시험의 경우 혼합고장을 제외한다면 하나의 모듈이 $(j-1)$개의 다른 모듈과 공통원인고장을 일으키는 사건의 총고장률의 비율은 $\alpha_j/\binom{7}{j-1}$이다. 그리고 8개의 모듈에서 j개가 공통원인고장을 일으키는 가짓수는 $\binom{8}{j}$이므로 8개의 모듈에서 j개가 공통원인고장을 일으키는 고장률의 비율은 $\binom{8}{j}\times\alpha_j/\binom{7}{j-1}$이다. 따라서 공통원인고장은 $j=6$, 7, 8로 $(\frac{8\alpha_6}{6}+\frac{8\alpha_7}{7}+\alpha_8)$으로 주어지고 <Table 5>의 작동요구 시에만 작동하는 시스템의 α_j의 평균값을 대입하면 $(\frac{8\alpha_6}{6}+\frac{8\alpha_7}{7}+\alpha_8)=0.014639\approx0.01$이다. 마찬가지로 비순차시험의 경우에 공통원인고장은 $\alpha_t=\sum_{j=1}^{8} j\alpha_j$라 하면 $8(\frac{\alpha_6+\alpha_7+\alpha_8}{\alpha_t})$으로 주어지고 <Table 5>의 작동요구 시에만 작동하는 시스템의 α_j의 평균값을 대입하면 $8(\frac{\alpha_6+\alpha_7+\alpha_8}{\alpha_t})=0.09407\approx0.09$이다. 따라서 순차시험과 비순차시험의 경우에 g값은 각각 0.01과 0.09으로 할 수 있다. 한편 Hirschberg *et al.*(1992)도 베타인자모형을 사용하는 경우에 보수적 관점에서 모수값 0.1의 사용을 제시하고 있다.

<Figure 2>는 g = 0.01과 g = 0.09 그리고 g = 0을 적용하여 24개월까지 운전시간에 따른 시스템 고장확률을 나타낸 것이다. 분석을 위해 고려한 운전시간을 24개월로 한 것은 현재 안전과 경제성을 위하여 발전소를 운전시간 18개월마다 예방정비하고 있기 때문이다. 그림에서 g = 0의 경우는 모듈들이 CCF가 없이 독립적으로 고장을 일으킬 때의 시스템의 불신뢰도를 나타내고 있다. 3개의 그래프는 시간이 경과함에 따라 불신뢰도가 거의 직선적으로 증가함을 보여준다. 또한 24개월까지의 모든 시점에서 g = 0을 기준으로 할 때 g = 0.09에서의 고장확률의 증가는 g = 0.01에서의 고장확률의 증가에 약 9배를 유지하고 있다.

한편 각 CCCG가 시스템의 불신뢰도에 미치는 영향을 알아보기 위하여 각 시점에서 독립고장만 있는 경우에 비하여 CCF를 고려했을 때 증가되는 불신뢰도를 구하고 불신뢰도의 증가에 각 CCCG가 끼치는 정도를 살펴본다. 24개월까지의 모든 시

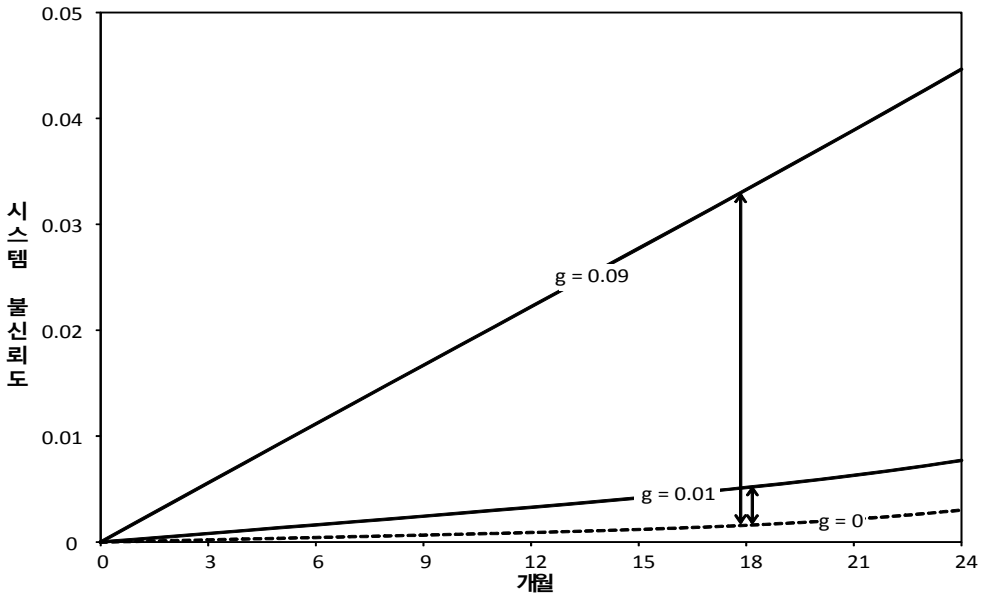

Figure 2. 전역 공통원인인자와 시스템의 불신뢰도

점에서 사용된 전역 공통원인인자에 관계없이 RIM으로 구성된 CCCG는 약 35%, BSM, CCM, EIM으로 구성된 CCCG들은 각각 약 22% 불신뢰도의 증가에 영향을 끼치는 것으로 나타났다. 따라서 4개의 CCCG 모두를 상세한 정량적 분석에 사용한다. 그런데 각 모듈로 구성된 CCCG가 시스템의 고장에 끼치는 영향의 비가 <Table 1>의 4종류의 모듈의 고장률의 비와 거의 일치하고 있는 이유는 각 CCCG에 대하여 지수고장분포를 가정할 때 고장률이 충분히 작으면 어느 정도 시간까지 불신뢰도 $F(t)$가 $F(t) \approx \lambda t$와 같이 고장률에 비례하기 때문인 것 같다.

3.2 상세한 정량적 분석

십여 년 전에 미국의 원자력 규제 위원회는 1980년부터 그 당시까지 기록된 장비와 관련된 고장 보고서들의 데이터를 수집하여 CCF 사건을 확인하고 분석하여 데이터베이스를 구축하였다(Marshall *et al*., 1998b). 이와 같이 CCF에 대한 데이터베이스가 개발되었음에도 불구하고 원전의 위험과 신뢰성 연구에서 관심 있는 모든 장비에 대하여 CCF의 분석을 위한 CCF 모형의 관련 모수값을 추정하는 것은 여전히 쉽지 않다. 그러므로 공학적 판단에 기초하여 모수값을 추정하는 것이 실질적으로 필요하다. 공통원인고장모형의 모수에 대한 주관적 추정 과정은 공통원인기본사건의 중요성에 따라서 단순한 한계값을 평가하는 것에서 부터 Paula and Parry(1990)의 원인-방어 행렬(Cause-Defense Matrix)과 Marshall *et al*.(1998a)의 부분적 모수화(Partial Parameterization)와 같은 기법을 필요로 하는 더욱 정교하고 구조적인 공학적 평가까지 있다. 그러나 어떠한 적용 절차에도 불구하고 추정의 결과는 숫자화 되어 나타나야 하므로 큰 불확실성을 수반하는 사건의 빈도에 대한 주관적 정량화일 뿐이다.

본 논문에서 다루는 원자로 보호시스템은 디지털 신호처리기(Digital Signal Processor)를 사용하여 새롭게 설계되고 있는 것으로 운전데이터가 전무하다. CCF를 분석하기 위한 모형은 여러 가지가 있으나 원자력 발전 분야에서는 CCF를 분석하기 위하여 구축된 데이터베이스가 알파인자모형을 적용하기 쉽도록 되어 있을 뿐만 아니라 발전소마다 다른 CCF를 반영하기 위한 베이지안 분석도 알파인자 모형이 용이하다. 따라서 CCF 분석에서 알파인자모형을 적용하고 잘 알려진 <Table 5>의 일반적 모수 추정값을 사용한다.

<Table 2>는 Relex Software의 결함나무 분석결과에서 스위칭설비를 제외하고 얻어진 총 1,004개의 최소 컷집합을 4종류의 사용되는 모듈에 따라 정리한 것이다. 여기서 모듈에 위첨자를 쓴 것은 주어진 모듈이 사용되는 개수를 나타낸 것이다. 예를 들면 BSM^3CCM^3는 8개의 중복된 BSM 중에서 특정한 3개와 8개의 중복된 CCM 중에서 특정한 3개를 합해서 총 6개의 모듈이 사용된 최소 컷집합을 나타낸다. <Table 2>를 보면 모든 최소 컷집합은 모듈의 종류에 상관없이 6개로 구성되어 있으며 4종류의 모듈이 모두 사용되는 최소 컷집합은 없다. 원자로 정지시스템과 안전설비 작동시스템에 모두 작동신호를 전달하지 못하는 컷집합은 52개, 원자로 정지시스템에 신호를 전달하지 못하는 컷집합은 476개이고 안전설비 작동시스템에 신호를 전달하지 못하는 컷집합도 476개이다.

한편 하나의 CCCG는 8개의 동일 모듈로 구성되어 있으므로 이 그룹에 속하는 하나의 모듈은 128개의 고장에 대한 기본사건을 가진다. 즉 기본사건들은 하나의 독립고장사건과 127개의 공통원인고장사건으로 구성되어 있다. 따라서 독립고장만으로 작성된 원래의 결함나무모형에서 각 기본사건을 128개의 고장사건이 OR 게이트로 연결된 새로운 사건으로 치환해야 CCF를 고려한 결함나무모형이 작성된다. 복잡한 시스템의 경우 Relex Software에서 이와 같은 방법은 번거로운 작업이므로

Table 2. 최소 컷집합에 대한 구성 모듈의 형태

원자로 정지시스템과 안전설비 작동시스템에 모두 작동신호 미전달			
구성 모듈의 형태	개수		
BSM^6	16		
CCM^6	4		
BSM^3CCM^3	32		
합	52		
원자로 정지시스템에 작동신호 미전달		안전설비작동시스템에 작동신호 미전달	
구성 모듈의 형태	개수	구성 모듈의 형태	개수
RIM^6	4	EIM^6	4
BSM^3RIM^3	32	BSM^3EIM^3	32
CCM^5RIM^1	24	CCM^5EIM^1	24
CCM^4RIM^2	60	CCM^4EIM^2	60
CCM^3RIM^3	80	CCM^3EIM^3	80
CCM^2RIM^4	60	CCM^2EIM^4	60
CCM^1RIM^5	24	CCM^1EIM^5	24
$BSM^3CCM^1RIM^2$	96	$BSM^3CCM^1EIM^2$	96
$BSM^3CCM^2RIM^1$	96	$BSM^3CCM^2EIM^1$	96
합	476	합	476

손쉽게 공통원인고장의 분석을 위한 메뉴가 있지만 CCCG의 크기 4까지만 가능하다. 따라서 독립고장만으로 작성된 원래의 결함나무를 분석한 <Table 2>를 이용하여 CCF를 고려한 최소 컷집합을 구하고 정량적 분석을 행한다.

예를 들면, <Table 2>에서 CCM^4RIM^2 형태의 최소 컷집합은 CCM 4개와 RIM 2개를 포함할 수 있는 선택된 3개 채널에서 트레인에 관계없이 RIM이 2개 선택되는 조합으로 구성되어 있다. 즉 CCM^4RIM^2 형태의 최소 컷집합은 ${}_4C_3 \cdot {}_6C_2 = 60$개이다. ccm_A1을 채널 1의 A 트레인에 있는 CCM의 고장을 나타낸다고 하자. CCM^4RIM^2 형태에 속하는 하나의 최소 컷집합 {ccm_A1, ccm_A2, ccm_B1, ccm_B2, rim_A3, rim_B3}에 대하여 살펴보자. 집합 내에서 ccm_A1은 독립고장이고 ccm_A2, ccm_B1, ccm_B2가 CCF를 일으키는 경우를 혼합고장(Mixed Failure)라고 한다. 이와 같이 동종의 모듈에 발생하는 혼합고장은 발생 가능성이 희박하므로 발생하지 않는다고 가정한다. 또한 ccm_A1, ccm_A2이 CCF이고 ccm_A2, ccm_B1, ccm_B2도 CCF가 발생하는 경우는 동일한 모듈 ccm_A2가 서로 다른 고장원인에 의하여 동시에 고장나는 경우로 역시 발생가능성이 희박하여 발생하지 않는다고 가정한다. <Table 3>은 CCM^4RIM^2 형태의 컷집합에서 공통원인고장을 고려하여 확장된 최소 컷집합 형태와 개수를 요약한 것이다. 표에서 ccm_4는 최소 컷집합 {ccm_A1, ccm_A2, ccm_B1, ccm_B2, rim_A3, rim_B3}에 속하는 4개의 CCM만 CCF를 일으키는 것이며 ccm_5는 최소 컷집합에 속하는 4개의 CCM과 이 최소 컷집합에 속하지 않는 ccm_A3, ccm_A4, ccm_B3, ccm_B4 중 하나의 CCM이 합해져서 5개가 공통으로 고장을 일으키는 것을 나타낸다. $(\text{ccm_1})^4$는 최소 컷집합에 속하는 4개의 CCM이 모두 독립적으로 고장을 일으키는 것을 나타낸다.

Table 3. CCM^4RIM^2에 대한 독립 및 공통원인고장 최소 컷집합

고장	최소 컷집합 형태 및 개수
독립	$((\text{ccm_1})^4, (\text{rim_1})^2) = 60$
공통원인	(ccm_4, rim_2) = 60, $((\text{ccm_1})^4$, rim_2) = 60, (ccm_4, $(\text{rim_1})^2$) = 60
공통원인	(ccm_4, rim_3) = 360, (ccm_5, rim_2) = 240, $((\text{ccm_1})^4$, rim_3) = 360, (ccm_5, $(\text{rim_1})^2$) = 240
공통원인	(ccm_4, rim_4) = 900, (ccm_5, rim_3) = 1440, (ccm_6, rim_2) = 360, $((\text{ccm_1})^4$, rim_4) = 900, (ccm_6, $(\text{rim_1})^2$) = 360
공통원인	(ccm_4, rim_5) = 1200, (ccm_5, rim_4) = 3600, (ccm_6, rim_3) = 2160, (ccm_7, rim_2) = 240, $((\text{ccm_1})^4$, rim_5) = 1200, (ccm_7, $(\text{rim_1})^2$) = 240
공통원인	(ccm_4, rim_6) = 900, (ccm_5, rim_5) = 4800, (ccm_6, rim_4) = 5400, (ccm_7, rim_3) = 1440, (ccm_8, rim_2) = 60, $((\text{ccm_1})^4$, rim_6) = 900, (ccm_8, $(\text{rim_1})^2$) = 60
공통원인	(ccm_4, rim_7) = 360, (ccm_5, rim_6) = 3600, (ccm_6, rim_5) = 7200, (ccm_7, rim_4) = 3600, (ccm_8, rim_3) = 360, $((\text{ccm_1})^4$, rim_7) = 360
공통원인	(ccm_4, rim_8) = 60, (ccm_5, rim_7) = 1440, (ccm_6, rim_6) = 5400, (ccm_7, rim_5) = 4800, (ccm_8, rim_4) = 900, $((\text{ccm_1})^4$, rim_8) = 60
공통원인	(ccm_5, rim_8) = 240, (ccm_6, rim_7) = 2160, (ccm_7, rim_6) = 3600, (ccm_8, rim_5) = 1200
공통원인	(ccm_6, rim_8) = 360, (ccm_7, rim_7) = 1440, (ccm_8, rim_6) = 900
공통원인	(ccm_7, rim_8) = 240, (ccm_8, rim_7) = 360
공통원인	(ccm_8, rim_8) = 60

따라서 CCM^4RIM^2 형태에 대하여 독립고장과 공통원인고장의 확률은 식 (3)과 같이 계산된다.

$$P(F) = P(\bigcup_{i=1}^{m} C_i) \approx \sum_{i=1}^{m} \prod_{j=1}^{k_i} P(E_{ij}) \tag{3}$$

여기서 $C_1, C_2, \cdots, C_m$은 최소 컷집합들이고 $C_i = \{E_{i1}, E_{i2}, \cdots, E_{ik_i}\}$이다. 즉 E_{ij}는 최소 컷집합 C_i의 j번째 기본사건이다. 식 (3)의 근사계산식은 최소 컷집합들이 서로 배반이며 더불어 최소 컷집합을 구성하는 기본사건들이 서로 독립이며 낮은 발생확률을 가질 때 잘 성립한다. 식 (3)의 근사계산식은 고장확률 $P(F)$에 대한 식 (4)의 부등식의 상계(Upper Bound)이다.

$$1-\prod_{i=1}^{m}\left[1-\prod_{j=1}^{k_i}P(E_{ij})\right]\le P(F)\le\sum_{i=1}^{m}\prod_{j=1}^{k_i}P(E_{ij}) \qquad (4)$$

식 (4)의 상계는 고장확률을 넉넉히 평가하는 보수적 관점을 가지므로 안전 및 신뢰성 평가에서 근사식으로 널리 사용되지만 경우에 따라 1을 능가할 수 있으며 주의 깊게 사용되어야 한다. Vesely(2002)는 기본사건의 발생확률이 0.1보다 작은 경우 결함나무에서 정상사건의 발생확률을 계산한 오차는 10% 이내에 있고 몇몇의 기본사건의 확률이 0.1보다 커도 대다수의 기본사건의 확률이 0.1보다 작으면 역시 오차가 10% 이내로 주어진다고 하였다. 그리고 근사계산의 정확도는 식 (4)의 하계(Lower Bound)를 계산해서 검토할 수 있다고 했다.

<Figure 3>은 $k_i = 4\sim7$, $P(E_{ij}) = 0.1$, $m = 1\sim10000$일 때 식 (4)의 부등식에서 상계값과 하계값을 구하여 상계값에 대한 상·하계값 범위, 즉 상대최대오차 백분율을 나타낸 것이다. $k_i = 1, 2, 3$에 대하여는 $m = 10, 100, 1000$보다 큰 경우 상계값이 1보다 커서 제외하였다. 그림을 보면 상대최대오차는 최소 컷집합의 크기가 4인 경우는 컷집합 2000개 이내에서, 최소 컷집합의 크기가 5, 6, 7인 경우는 컷집합 10000개 이상에서도 10%를 넘지 않는다.

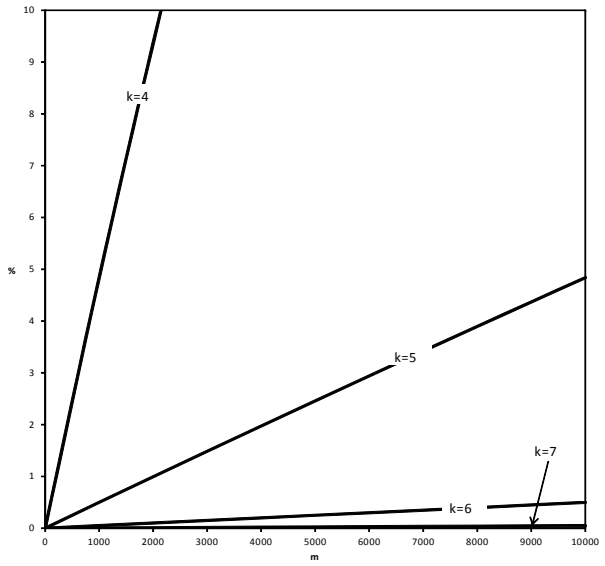

Figure 3. 근사계산의 상대최대오차 백분율

식 (3)을 이용하여 <Table 3>에 주어진 CCM^4RIM^2 형태에 대하여 독립고장과 공통원인고장의 확률을 기본적 모수모형으로 나타내면 식 (5)와 같다.

$$60\left(Q_1^C\right)^4\left(Q_1^R\right)^2+60Q_4^CQ_2^R+60\left(Q_1^C\right)^4Q_2^R \qquad (5)$$
$$+60Q_4^C\left(Q_1^R\right)^2+\cdots+60Q_8^CQ_8^R$$

여기서 Q_1^C은 하나의 CCM의 독립고장확률을 Q_4^C은 하나의 CCM이 다른 3개 CCM과 공통으로 고장을 일으키는 확률을 나타내며 RIM의 경우도 위첨자만 다를 뿐 같은 의미를 나타낸다.

CCM 8개가 CCCG이므로 CCF를 고려하면 이 그룹에 속한 임의의 하나의 CCM의 총고장률 λ_T^C는 순차시험의 경우 식 (6)과 같다.

$$\lambda_T^C=\sum_{j=1}^{8}\binom{7}{j-1}\lambda_j^C \qquad (6)$$

여기서 λ_1^C은 임의의 하나의 CCM의 독립고장의 고장률이며 λ_j^C $(j\ge2)$는 CCCG에서 임의의 j개의 CCM이 동시에 고장나는 공통원인고장의 고장률을 나타낸다.

한편 알파인자모형의 모수 α_j는 CCCG의 부품들이 전체 고장 중에 j개가 CCF를 일으키는 빈도(비율)이고 λ_j^C은 식 (7)과 같이 주어진다.

$$\lambda_j^C=\frac{1}{\binom{7}{j-1}}\alpha_j\lambda_T^C, \qquad j=1,\cdots,8 \qquad (7)$$

따라서 Q_j^C는 식 (8)과 같이 주어진다.

$$Q_j^C=1-e^{-\lambda_j^Ct} \qquad (8)$$

RIM 8개에 대하여도 식 (6), 식 (7), 식 (8)과 유사한 식이 성립하고 Q_j^R가 구해지며 식 (8)의 Q_j^C과 더불어 식 (5)에 대입하여 계산하면 CCM^4RIM^2 형태의 독립고장과 공통원인고장의 확률을 구할 수 있다. <Table 2>에 주어진 모든 구성 모듈의 형태에 대하여 계산한 고장확률의 합에 고장률이 $1.0\times10^{-7}/h$인 스위칭설비의 고장확률을 합하면 4개의 CCCG이 존재하는 경우에 시스템의 불신뢰도를 구할 수 있다.

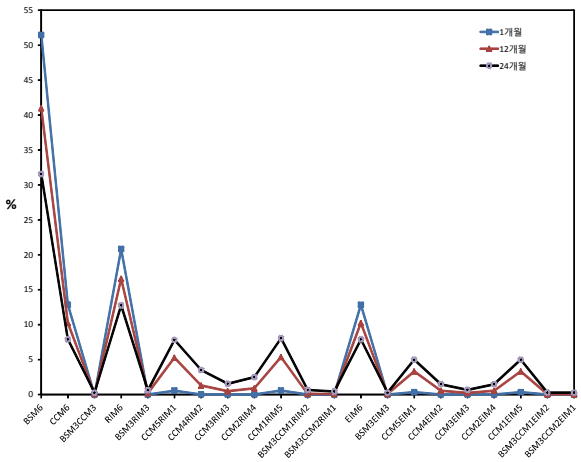

Figure 4. 최소 컷집합 형태가 공통원인고장에 미치는 영향

<Figure 4>는 <Table 5>의 연속적으로 작동하는 시스템에 대한 알파인자의 평균값을 사용하여 <Table 2>에 주어진 구성 모듈의 형태가 운전시간에 따라 시스템의 공통원인고장확률에 미치는 영향을 백분율로 나타낸 그래프이다. BSM^6, CCM^6, RIM^6, EIM^6과 같이 동종 모듈의 최소 컷집합 형태는 운전시간의 증가에 따라 영향력이 감소하고 이종 모듈이 혼합된 최소 컷집합 형태에서는 정도의 차이가 있지만 운전시간의 증가에 따라 영향력이 증가하고 있다. 이것은 운전시간의 경과에 따라 동종 모듈이 6개 이상 동시에 고장 나는 가능성을 작아지는 반면에 이종 모듈들이 조합하여 6개 이상이 동시에 고장 나는 가능성은 커진다는 것을 의미한다.

<Table 5>의 연속적으로 작동하는 시스템에 대한 알파인자의 평균값을 사용하여 원자로 보호시스템에 대한 불신뢰도의 계산 결과를 보여주는 것이 <Table 4>이다. (a)열의 독립고장확률은 각 모듈의 총고장률 $\lambda_T^{\bullet}$를 사용하여 시스템의 고장확률을 구한 것으로 시스템이 공통원인고장이 없이 독립고장만 일으키는 경우에 시스템의 불신뢰도이다. 한편 각 모듈의 총고장률 $\lambda_T^{\bullet}$에 식 (7)과 같이 $\alpha_j/\binom{7}{j-1}$을 곱하여 얻어진 고장률 $\lambda_j^{\bullet}$들을 사용하여 시스템의 고장확률을 구한 것이 (b)열의 총고장확률이다. 즉 시스템에 독립고장과 공통원인고장이 발생하는 경우에 시스템의 불신뢰도이다. (c)열과 (d)열은 (b)열의 총고장확률을 독립고장확률과 공통원인고장확률로 분해한 것이다. 특히 총고장확률 중 공통원인고장확률이 차지하는 비중이 상당히 큰데 이 비율을 보여주는 것이 (e)열로 약 90% 정도를 공통원인고장이 차지하고 있다. 이와 같이 공통원인고장이 중요한 이유는 시스템이 노화하지 않은 상태에서 시스템을 고장나게 하는 주요한 원인이 된다는 것이다. (f)열은 식 (3)의 근사계산의 최대상대오차를 평가하기 위하여 식 (4)의 하계식을 이용하여 총고장확률을 계산한 값이다. 최대상대오차는 개월이 증가에 따라 점점 커지지만 24개월 시점에서 약 1.2%이다. 한편 (b)열과 (a)열의 값의 차이는 시스템에 대하여 공통원인고장을 무시하고 독립고장만 발생한다고 하면 시스템의 불신뢰도를 과소평가하게 되는데 그 크기를 나타내며 이를 그래

Table 4. 시스템의 불신뢰도 계산 결과

개월	(a) 독립 고장 확률	(b) 총 고장 확률	(c) 공통 원인 고장 확률	(d) 독립 고장 확률	(e) 공통 원인 고장 확률(c) ÷총 고장 확률(b)	(f) 식 (4)의 하계값 총 고장 확률
0	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000
1	0.000073	0.000727	0.000654	0.000073	0.899619	0.000727
2	0.000146	0.001481	0.001335	0.000146	0.901441	0.001480
3	0.000219	0.002263	0.002044	0.000219	0.903238	0.002261
4	0.000292	0.003074	0.002782	0.000292	0.905009	0.003070
5	0.000365	0.003915	0.003550	0.000365	0.906758	0.003908
6	0.000438	0.004786	0.004348	0.000438	0.908484	0.004777
7	0.000512	0.005691	0.005179	0.000512	0.910027	0.005678
8	0.000587	0.006630	0.006043	0.000587	0.911457	0.006612
9	0.000663	0.007603	0.006941	0.000662	0.912930	0.007580
10	0.000741	0.008615	0.007876	0.000739	0.914215	0.008584
11	0.000821	0.009666	0.008847	0.000819	0.915274	0.009628
12	0.000906	0.010761	0.009858	0.000903	0.916086	0.010714
13	0.000996	0.011900	0.010909	0.000991	0.916722	0.011842
14	0.001093	0.013087	0.012002	0.001085	0.917091	0.013016
15	0.001199	0.014326	0.013138	0.001188	0.917073	0.014241
16	0.001317	0.015619	0.014319	0.001300	0.916768	0.015519
17	0.001448	0.016972	0.015547	0.001425	0.916038	0.016854
18	0.001595	0.018388	0.016824	0.001564	0.914942	0.018249
19	0.001763	0.019872	0.018150	0.001722	0.913347	0.019711
20	0.001954	0.021429	0.019529	0.001900	0.911335	0.021242
21	0.002172	0.023065	0.020962	0.002103	0.908822	0.022850
22	0.002422	0.024785	0.022450	0.002335	0.905792	0.024539
23	0.002708	0.026596	0.023997	0.002599	0.902278	0.026314
24	0.003034	0.028502	0.025603	0.002899	0.898288	0.028181

Table 5. CCCG의 크기 8에 사용되는 모수추정값

	작동요구 시에만 작동하는 시스템					
알파인자	a	b	평균값	0.05분위수	0.5분위수	0.95분위수
α_1	97.6507	4.349	0.95736	9.20×10^{-1}	9.60×10^{-1}	0.984
α_2	1.1118	100.888	0.01090	7.25×10^{-4}	7.91×10^{-3}	3.13×10^{-2}
α_3	0.7915	101.209	0.00776	2.07×10^{-4}	4.87×10^{-3}	2.52×10^{-2}
α_4	0.6253	101.375	0.00613	6.92×10^{-5}	3.34×10^{-3}	2.17×10^{-2}
α_5	0.4417	101.558	0.00433	8.51×10^{-6}	1.76×10^{-3}	1.74×10^{-2}
α_6	0.2581	101.742	0.00253	6.09×10^{-8}	4.74×10^{-4}	1.21×10^{-2}
α_7	0.1969	101.803	0.00193	1.59×10^{-9}	1.93×10^{-4}	1.00×10^{-2}
α_8	0.9241	101.076	0.00906	3.82×10^{-4}	6.12×10^{-3}	2.78×10^{-2}
	연속적으로 작동하는 시스템					
알파인자	a	b	평균값	0.05분위수	0.5분위수	0.95분위수
α_1	$0.22930\sim4.586\times10^{11}$	$0.005\sim1\times10^{10}$	0.97866	$0.99811\sim0.97866$	$1\sim0.97866$	$1\sim0.97866$
α_2	1.1222	204.786	0.00545	3.68×10^{-4}	3.96×10^{-3}	1.56×10^{-2}
α_3	0.7964	204.461	0.00388	1.05×10^{-4}	2.43×10^{-3}	1.26×10^{-2}
α_4	0.6280	204.266	0.00307	3.51×10^{-5}	1.67×10^{-3}	1.08×10^{-2}
α_5	0.4431	204.222	0.00217	4.32×10^{-6}	8.80×10^{-4}	8.67×10^{-3}
α_6	0.2585	204.089	0.00127	3.09×10^{-8}	2.37×10^{-4}	6.06×10^{-3}
α_7	0.1971	204.052	0.00097	8.02×10^{-10}	9.65×10^{-5}	5.00×10^{-3}
α_8	0.9314	204.588	0.00453	1.94×10^{-4}	3.06×10^{-3}	1.39×10^{-2}

프로 나타낸 것이 <Figure 5>이다. 따라서 원자로 보호시스템처럼 신뢰도를 높이기 위하여 구성품을 중복하여 설계된 시스템을 공통원인고장을 무시하고 독립고장만으로 신뢰도를 추정한다면 상당히 과소평가한 결과를 얻게 된다는 것을 보여준다. 한편 EPRI-URD에 의하면 원자로 보호시스템의 신뢰성 목표는 평균고장시간이 50년이다. 이와 같은 신뢰성 목표를 달성하기 위한 고장률은 $2.238\times10^{-6}/h$로 운전시간에 따른 고장

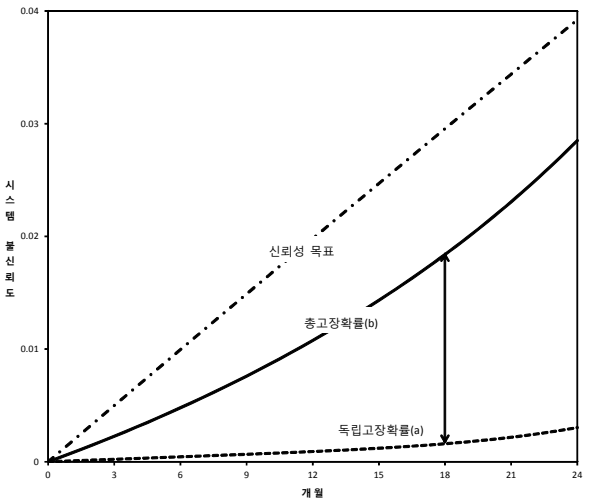

Figure 5. 시스템 불신뢰도의 과소평가

확률의 그래프를 보여주는 것이 그림에서 쇄선이다. 이를 보면 CCF가 존재하지만 24개월 이내에는 신뢰성 목표를 충분히 만족하고 있다.

Mosleh *et al.*(1998)은 CCF 데이터베이스를 분석하여 크기 8의 CCCG에서 식 (7)의 계산에 사용되는 알파인자모형의 모수 α_i에 대한 사전분포로 베타분포를 가정하고 추정된 베타분포의 평균값, 0.05분위수, 0.5분위수, 0.95분위수를 추정하였다. <Table 5>의 작동요구 시에만 작동하는 시스템에 주어진 값들이 그것이다. 사전 분포는 운전데이터를 이용하여 알파인자모형의 모수의 베이지안 추정값을 구하기 위하여 사용한다. 그러나 디지털 원자로 보호시스템에 대한 운전데이터가 없으므로 사전 분포에 대하여 주어진 추정값을 그냥 사용한다.

또한 Mosleh *et al.*(1998)은 운전 중 계속 사용되는 시스템의 공통원인고장빈도는 평상 시 대기상태로 있다가 작동요구 시에만 작동하는 시스템의 공통원인고장빈도보다 작아서 <Table 5>의 작동요구 시에만 작동하는 시스템에 주어진 $\alpha_2\sim\alpha_8$에 대하여 추정값의 반을 사용하는 것을 추천한다. 이에 대한 이유는 작동요구 시에만 작동하는 시스템의 경우는 고장이 탐지되는 것이 작동요구 시에만 가능하므로 작동요구 사이 시간에 고장을 일으킨 것은 구별되지 못하므로 공통원인고장으로 인식되지만 연속적으로 사용되는 시스템의 경우는 고장이 발생 즉시 탐지되므로 동시에 고장을 일으키지 않으면 공통원인고장으로 인식되지 않기 때문이다.

원자로 보호시스템은 운전 중 계속 작동하며 원자로를 체크하고 이상 발생 시에 후속 시스템의 작동을 지시하는 시스템으로 <Table 5>의 연속적으로 작동하는 시스템에 주어진 $\alpha_2 \sim \alpha_8$의 값을 공통원인고장빈도의 평균값과 0.05분위수, 0.5분위수, 0.95분위수로 갖는다. 이것은 작동요구 시에만 작동하는 시스템의 공통원인고장빈도 $\alpha_2 \sim \alpha_8$에 대한 평균값과 0.5분위수를 정확히 반으로 하는 베타분포들을 구한 후, 이 베타분포로부터 0.05분위수와 0.95분위수를 구한 것이다. 이와 같이 구해진 0.05분위수와 0.95분위수는 작동요구 시에만 작동하는 시스템에 주어진 0.05분위수와 0.95분위수의 거의 반에 해당하는 값으로 된다. 한편 연속적으로 작동하는 시스템의 독립고장빈도 평균값 $\alpha_1 = 0.97866$은 전체고장빈도의 합이 1이 되도록 하여 구해진 것이다. 이 때 평균이 0.97866인 베타분포에 대하여 모수가 $a = 0.229302$, $b = 0.005$에서 $a = 4.586 \times 10^{11}$, $b = 1 \times 10^{10}$까지 변할 때 0.05분위수는 0.99811에서 0.97866까지, 0.5분위수와 0.95분위수는 1에서 0.97866까지 감소되며 변화된다. 표의 연속적으로 작동하는 시스템의 α_1행에 주어진 값의 범위는 이를 나타내고 있다.

한편 시스템의 불신뢰도에 대한 점추정에는 알파인자의 평균값을 일반적인 모수값으로 사용한다. 그러나 CCF 분석을 위해 사용되는 모든 모형에서 모수값의 결정에 많은 불확실성이 존재한다. 알파인자모형에서는 모수의 0.05분위수, 0.5분위수, 0.95분위수를 사용하여 시스템의 불신뢰도에 대한 불확실성을 평가한다. <Figure 6>은 알파인자모형에서 3개의 분위수와 평균값을 사용했을 때 원자로 보호시스템의 불신뢰도를 보여주고 있다. 0.05분위수, 0.5분위수, 0.95분위수에 대하여는 독립고장빈도 α_1은 상한값과 하한값의 각각 적용하였다. 각 분위수의 이 극단값에 대하여 시스템의 고장확률의 차이는 거의 없음을 보여주고 있다. 0.05분위수의 경우에 독립고장빈도로 상한값 0.99811을 사용한 시스템의 불신뢰도는 모든 운전시점에서 평균값에 기초한 불신뢰도의 약 10%를 차지하며 매우 작다. 반면에 0.95분위수에서 독립고장빈도로 상한값 1을 사용한 시스템의 불신뢰도는 평균값에 기초한 불신뢰도의 약 300%를 차지하고 있다. 따라서 시스템의 불신뢰도에 대한 불확실성이 상당히 큼을 알 수 있다. 0.5분위수에서의 불신뢰도가 평균값에서의 불신뢰도보다 작고, 0.95분위수에서 불신뢰도보다 0.05분위수에서의 불신뢰도에 가까운 것은 <Table 4>에서 보여주듯이 공통원인고장확률이 총고장확률에 큰 비중을 차지하는 가운데 공통원인고장빈도를 나타내는 $\alpha_2 \sim \alpha_8$ 모수의 사전 분포가 베타분포로서 오른쪽으로 치우친 모양을 하고 있기 때문이다.

한편 공통원인고장빈도 $\alpha_2 \sim \alpha_8$에 대한 시스템의 불신뢰도의 민감도를 살펴보기 위하여 <Table 5>의 작동요구 시에만 작동하는 시스템의 알파인자 $\alpha_2 \sim \alpha_8$의 평균값을 1, 0.75, 0.5, 0.25배 하고 알파인자의 합이 1이 되도록 α_1을 보정한 네 가지 경우에 대한 시스템의 불신뢰도를 나타낸 것이 <Figure 7>이다. 0.5배 한 경우는 연속적으로 작동하는 시스템의 경우이다. 그림을 살펴보면 모든 시점에서 각각의 경우에 독립고장의 불신뢰도인 점선을 차감한 값은 거의 4 : 3 : 2 : 1의 비로 나타나고 있다. 즉 공통원인고장빈도 $\alpha_2 \sim \alpha_8$의 감소율에 비례하여 비슷한 비율로 불신뢰도도 감소되고 있다. 따라서 시스템의 불신뢰도가 알파인자 $\alpha_2 \sim \alpha_8$의 변화에 대하여 상당히 민감하다.

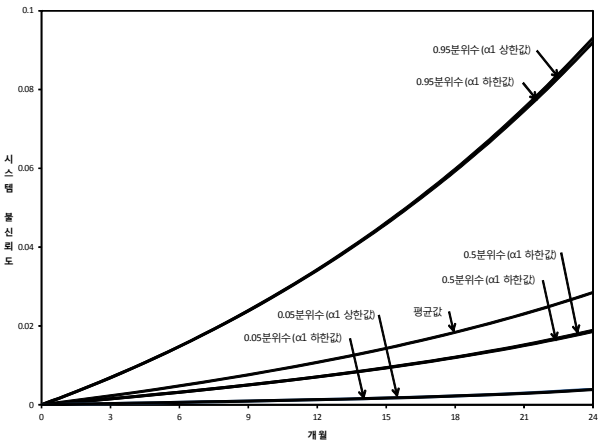

Figure 6. 모수의 불확실성을 고려한 시스템 불신뢰도

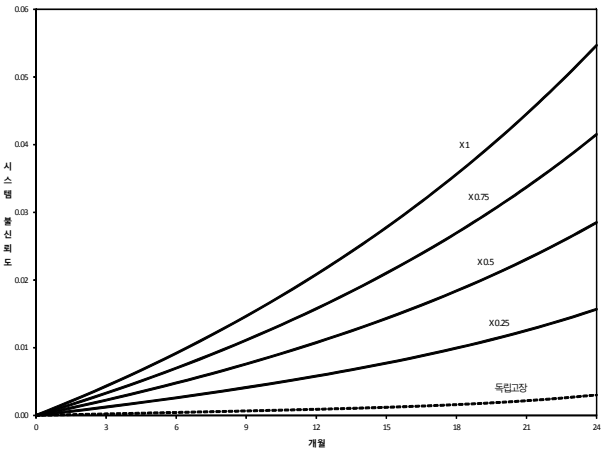

Figure 7. 공통원인고장빈도의 변화에 따른 시스템의 불신뢰도

<Figure 8>은 알파인자모형과 베타인자 모형에서 $g = 0.035$, 0.04, 0.045, 0.05, 0.055을 사용하여 원자로 보호시스템의 불신뢰도를 평가한 그래프이다. 알파인자모형은 불신뢰도가 아래로 볼록한 형태로 증가하는데 반하여 베타인자 모형은 거의 직선적으로 증가하고 있다. 따라서 베타인자 모형은 알파인자모형의 근사모형으로 사용가능함을 알 수 있다. 그러나 공통원인고장에 사용되는 다른 여러 모형과 마찬가지로 모수값의 정확한 추정이 문제가 된다. 한편 24개 개월 시점의 불신뢰도 값들에 대하여 평균절대편차(Mean Absolute Deviation; MSD)와 평균제곱오차(Mean Squared Error:MSE)를 구해본 결과 각각 $g = 0.045$와 0.05가 알파인자모형을 적용한 결과와 잘 일치되었다.

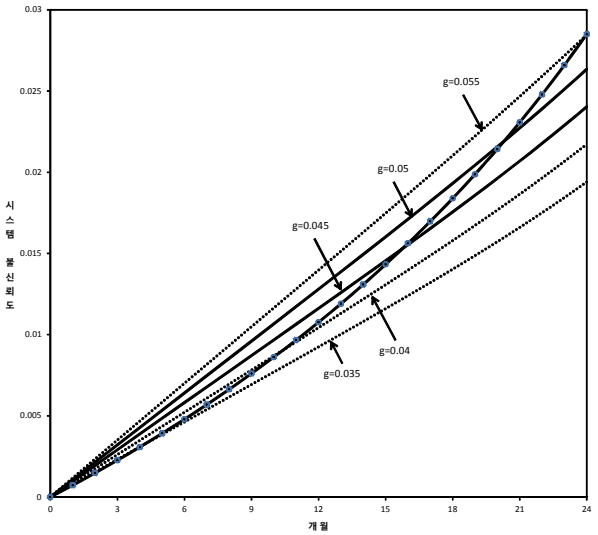

Figure 8. 베타인자모형을 사용한 근사적 불신뢰도

4. 결 론

본 논문에서는 원자력 발전소의 안전성과 경제성을 동시에 추구하기 위하여 구성품의 중복 개념을 도입하여 설계된 원자로 보호시스템에 대하여 공통원인고장에 대한 분석을 행하였다. 공통원인고장은 구성품의 중복설계의 장점을 감쇄시키는 고장사건으로 구성품이 중복 사용되어 있는 시스템의 신뢰성을 평가할 때 반드시 고려되어야 한다. 원자로 보호시스템은 독립된 4개 채널의 이중화 구조로 4종류의 모듈이 8개씩 중복 사용되고 있다. 알파인자모형을 사용하여 일반적인 모수값에 기초한 운전시간 24개월까지의 결과는 공통원인고장확률이 총 고장확률의 약 90%를 차지하고 있어 공통원인고장의 중요성을 알 수 있었다.

시스템의 불신뢰도에 대한 불확실성을 평가하기 위하여 알파인자모수의 0.05, 0.5, 0.95분위수를 사용하여 불신뢰도를 평가한 결과 불확실성이 상당히 크게 나타났다. 0.05분위수를 사용한 시스템의 불신뢰도는 평균값에 기초한 불신뢰도의 약 0.1배, 0.95분위수를 사용하여 평가된 시스템의 불신뢰도는 평균값에 기초한 불신뢰도의 약 3배를 차지하고 있다. 향후 모듈의 공통원인고장에 데이터가 축적되어 이를 반영한 더욱 정확한 베이지안 모수추정값을 사용할 수 있다면 불확실성이 작아져서 좀 더 정확히 시스템의 불신뢰도를 추정할 수 있을 것이다.

참고문헌

Eide, S. A. *et al*. (1999), *Westinghouse Reactor Protection System Unavailability*, INEEL

Ericson, C. A. (2005), *Hazard Analysis Techniques for System Safety*, Wiley-Interscience.

Fleming, B. W. and Mosleh, A. (1985), Common-Cause Data Analysis and Implications in System Modeling, *Proceedings of the International Topical Meeting on Probabilistic Safety Methods and Applications*, 1(3/1-3)/12).

Hirschberg, S. *et al*. (1992), *Procedures for Conducting Common Cause Failure Analysis in Probabilistic Safety Assessment*, IAEA.

Kamyab, S. H. *et al*. (2010), Evaluating the Reliability of AP1000 Passive Core Cooling Systems with Risk Assessment Tool, *Proceedings of the International Multiconference of Engineers and Computer Scientists*, 3, 1668-1673.

Kong, M. B. and Lee, S. Y. (2010), Safety Assessment for the Design of Reactor Protection System of Nuclear Power Plant, *IE Interfaces*, 23(1), 68-77.

Marshall, F. M. *et al*. (1998a), *Common Cause Failure Data Collection and Analysis System-Event Definition and Classification, NUREG/CR-6268*, U. S. NRC, 2.

Marshall, F. M. *et al*. (1998b), *Common Cause Failure Data Collection and Analysis System-Software Reference Manual, NUREG/CR-6268*, U. S. NRC, 4.

Mosleh, A. *et al*. (1988), *Procedure for treating Common Cause Failures in Safety and Reliability Studies, NUREG/CR-4780*, U. S. NRC, I and II.

Mosleh, A. *et al*. (1998), *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*, *NUREG/CR-5485*, U. S. NRC .

Paula, H. M. and Parry, G. W.(1990), *A Cause-Defense Approach to the Understanding and Analysis of Common-Cause Failures, NUREG/CR-5460,* U. S. NRC.

Rutledge, P. J. and Mosleh, A. (1995), Dependent-Failures in Spacecraft: Root Causes, Coupling Factors, Defenses, and Design Implications, *RAMS*, 337-342.

Shooman, M. L. (2002), *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*, John Wiely and Sons, Inc.

Tang, Z. and Dugan, J. B. (2004), An Integrated Method for Incorporating Common Cause Failures in System Analysis, *RAMS*, 610-614.

Vesely, W. E. *et al*. (2002), *Fault Tree Handbook with Aerospace Applications,* NASA.

공 명 복
서울대학교 산업공학과 학사
한국과학기술원 산업공학과 석사
한국과학기술원 산업공학과 박사
현재 : 울산대학교 산업경영공학부 교수
관심분야 : 응용통계, 신뢰성공학, 안전공학

이 상 용
울산대학교 산업대학원 석사
울산대학교 산업공학과 박사
현재 : 포뉴텍 R&D 센터 센터장
관심분야 : 신뢰성공학, 기기내환경 검증,
설비보전, 원전수명관리