IE Interfaces
Vol. 23, No. 1, pp. 68-77, March 2010.

원자력 발전소 디지털 원자로 보호시스템의 설계에 대한 안전성 평가

공명복[1] · 이상용[2†]

[1]울산대학교 산업경영공학부 / [2]삼창기업(주) 원자력사업본부

Safety Assessment for the Design of Digital Reactor Protection System of Nuclear Power Plant

Myung-Bock Kong[1] · Sang-Yong Lee[2]

[1]Department of Industrial Engineering, University of Ulsan, Ulsan, 680-749
[2]Nuclear Power Division Head Office, SAMCHANG ENTERPRISE CO., LTD, Ulsan, 689-871

Digital reactor protection system which consists of many identical modules, is fault- tolerant to provide high safety. The modules themselves including DSP(digital signal processing) card are also fault-tolerant in nature. This paper assesses the safety for being-designed digital reactor protection system of 2-out-of-4 G structure with lockout. Some interesting design alternatives are compared. Fault tree analysis for assessing system safety is performed by Relex software. The selected reactor protection system fully satisfies EPRI-URD stipulation of mean failure time of 50 years.

Keyword: reactor protection system, DSP, 2-out-of-4 G structure with lockout, fault tree, safety assessment

1. 서 론

디지털 기술의 급격한 발전으로 인해 점차 원자력 발전소 안전 시스템에도 디지털 기기들이 도입되어 활용되고 있다. 그러나 일반 산업체와는 달리 원자력 발전소에서 발생하는 사고의 여파는 일반 공중에게 방사능 누출과 방사성 물질에 의한 피해를 입힐 수 있는 가능성을 내재하고 있다. 이러한 가능성을 배제하기 위하여 디지털 안전시스템은 설정된 사상에 대해서 첫째, 원자로 냉각재 압력경계의 건전성을 보장하고 둘째, 원자로를 정지시키고 원자로가 안전한 정지조건을 만족하는 것을 보장하고 셋째, 원자로 밖으로 누출되는 사고에 대해서도 그 피해를 최소화하거나 방지할 수 있음을 보장해야 한다. 따라서 시스템 개발 시 많은 구체적인 규제 요건의 적용을 받으며 이는 확보된 안전성이나 신뢰성의 정확한 추정을 필요로 한다.

국내에 현재 가동 중이거나 건설 중인 원자력 발전소 원자로 보호시스템은 해외 사업자가 공급한 제품으로 설계에 대한 안전성 및 신뢰성분석 결과만 제공되고 있다. 따라서 발전소 전체의 품질과 안전성을 예측하는 확률적 안전성 평가(PSA)가 일관성 있고 정확하게 이루어지지 못해 안전의 확보에 어려움을 겪고 있다. 또한 해외에서 개발된 기존의 디지털 안전시스템의 플랫폼은 주로 PLC를 기반으로 개발되어지고 있다. 그러나 개발 중인 일체형 원자로의 디지털 원자로 보호시스템은 원천기술의 확보와 수출을 목표로 DSP를 기반으로 플랫폼을 개발하고 설계기술의 일환으로 설계단계에서부터 신뢰성 평가를 도입하여 설계 신뢰성을 높이고자한다. 시스템의 설계단계에서 신뢰성 평가는 주어진 임무시간 동안 시스템의 신뢰성

†연락저자 : 이상용 이사, 689-871 울산광역시 울주군 웅촌면 고연리 974-1 번지 삼창기업(주) 원자력 사업 본부, Fax : 052-260-7230, E-mail : lsy010@samchang.com
투고일(2009년 09월 04일), 심사일(1차 : 2009년 12월 04일, 2차 : 2010년 01월 17일), 게재확정일(2010년 01월 21일).

을 예측하거나 시스템을 구성하는 부품들의 상충관계를 파악하거나 최적의 시스템을 선택하기 위한 여러 대안들을 평가하기 위하여 사용된다.

결함나무분석은 시스템의 신뢰성 및 확률적 안전성 평가를 위해 사용되는 가장 중요한 논리적 및 확률적 기법의 하나이다(Vesely, 2002). 여기서 결함나무란 시스템에 바람직하지 못한 사상(정상사상)이 발생했다고 가정하고 하위 시스템의 어떠한 고장모드(기본사상)가 정상사상의 원인이 되는지 게이트를 사용하여 부울논리로 표현한 것이다. 전통적으로 결함나무에 대한 분석은 정성적 분석과 정량적 분석으로 구성된다. 정성적 분석은 정상사상을 발생시키는 기본사상들의 최소컷집합을 구하는 것이며 정량적 분석은 정성적 분석에 기초하여 주어진 기본사상의 발생확률로부터 정상사상의 발생확률을 구하는 것이다. 그러나 기본사상의 수가 많은 경우에는 최소컷집합의 수가 기하급수적으로 증가하여 이들을 구하는데 어려움이 있고 정상사상의 발생확률을 또한 근사적으로 구하게 된다. 따라서 정량적 분석에서 최소컷집합을 이용하지 않는 이진의사결정그림을 이용하여 정확한 정상사상의 발생확률을 구하는 방법이 연구되었다(Gulati *et al*., 1997; Reay *et al*., 2002).

또한 기본사상의 발생에 특정한 순서적인 관계가 존재하거나 기능적으로 종속되거나 대기중복 부품이 존재하는 경우에 전통적인 부울논리의 게이트 외에 기본사상들 사이에 동적인 특성을 표현하는 동적 게이트를 추가하여 시스템을 쉽게 이해할 수 있는 동적결함나무 모형이 개발되어 시스템분석에 사용되고 있다(Amari *et al*., 2003; Dugan *et al*., 1992; Vesely, 2002). 기본사상의 동적인 특성을 모형화하기 위한 다른 방법으로 부울논리가 적용된 마코프과정 모형(Bouissou *et al*., 2003)이나 동적베이지안네트워크 모형(Montani *et al*., 2006)등이 사용되고 있으나 안전성 분석가들에게 익숙하지 않고 시스템을 이해하기 쉽게 표현하기도 어렵다.

한편 동적결함나무에 대한 정량적 분석에서 대형화된 나무는 여러 개의 단순한 부나무로 나누어서 분석하는 방법이 효율적이라고 알려져 있다. 부나무로 나누는 방법으로 많이 이용되는 방법은 Dutuit *et al*.(1996)의 선형시간 알고리즘이다. Dugan *et al*.(2000)은 동적결함나무를 여러 개의 부나무로 나누었을 때 부나무의 여러 특성에 따라 효율적인 분석방법을 제시하고 있다.

본 연구는 원자력 발전소의 안전한 운용에 필수적인 원자로 보호시스템의 설계 및 제작 국산화를 위해 개발한 그 시작품인 디지털 시스템에 대하여 사용된 중복설계에 의한 내결함성(fault tolerance)을 평가하기 위하여 (동적)결함나무모형을 사용하여 안전성을 분석하였다. 이 시스템은 고장이 발생한 채널을 폐쇄(lockout)하고 운용하는 것이 가능하며 시스템을 구성하는 모듈들이 또한 내결함성을 가지고 있다. 원자로 보호시스템은 원자로의 작동에 이상이 발생했을 때 원자로를 정지시키며 정지된 상태를 지속하고 방사능 물질의 확산을 방지하는 것으로 원자로의 안전한 운용에 가장 중요한 시스템이다. 내결함성(Koren *et al*., 2007)기술은 결함의 발생을 감지하고, 결함의 위치를 찾아내고, 결함을 회복하여 시스템이 고장에 이르지 않도록 하는 방법이다. 물론 경우에 따라서는 회복된 시스템이 완전한 성능을 보이지는 않지만 고장은 아니므로 안전성이 특히 강조되는 시스템의 경우에 유용하게 사용된다. 과거에는 내결함성을 갖게 하기 위한 중복설계는 하드웨어의 추가적인 비용을 발생시키므로 사용이 제한되었으나 제작기술의 발달로 하드웨어의 비용이 감소되어 많이 사용되고 있고 앞으로 더욱 사용이 증가될 것이다. Siewiorek *et al*.(1992)은 시스템의 운용환경이 열악하고, 운용자의 경험이 부족하고, 시스템의 수리비용이 증가하거나, 시스템의 대형화에 따라 내결함성 기술 적용이 더욱 필요하다고 하였다.

논문의 구성은 제 2장에서는 디지털 원자로 보호시스템에 대한 구성모듈과 기능 및 구조, 제 3장에서는 디지털 원자로 보호시스템의 결함나무 모형화, 제 4장에서는 작성된 결함나무에 대하여 안전성 분석을 다룬다. 분석은 신뢰성 분석 소프트웨어로 널리 알려진 Relex를 이용하여 분석하였으며 제 5장은 결론 및 향후 연구과제에 대하여 기술하였다.

2. 원자력 발전소 디지털 원자로 보호시스템

원자력 발전소 원자로 보호시스템은 원자로 노심의 건전성 및 원자로 냉각재시스템의 압력경계값을 안전하게 유지하는 기능을 수행한다. 또한 시스템은 원자로에 이상상태가 발생하여 입력신호가 설정값에 도달하게 되면 원자로 제어봉의 입력전원을 자동으로 차단하여 원자로반응을 정지시킴과 동시에 안전설비를 작동시켜 사고의 확산을 방지하는 기능을 작동시키는 논리 구현 장치이다. 따라서 원자로 보호시스템의 신뢰성은 원자력 발전소 가동시 안전과 직접 관계되는 중요한 요소이며 원자로 보호시스템의 고장으로 인하여 원하지 않는 원자로 불시정지도 발생하지 않아야 한다. 최근에 원자력 발전소에서 아날로그 설비는 관련 부품의 단종으로 유지 및 보수가 불가능하고 전자기술이 디지털화함에 따라 발전소 비안전시스템 뿐만 아니라 안전시스템에도 디지털 설비를 사용하고 있다. 그러나 원자로 디지털 보호시스템은 아직 예측하지 못한 고장의 발생을 고려하여 큰 내결함성을 갖도록 중복설계와 수동 작동 시스템을 병행하여 채택하고 있다.

2.1 디지털 원자로 보호시스템의 구성모듈과 기능

원자력 발전소 디지털 원자로 보호시스템은 동일기기에 의한 다중임무라는 디지털 기기의 특성에 따라 4가지 모듈로 구성되어 있다. 다음은 보호시스템의 구성모듈과 그 기능을 간단히 요약한 것이다.

(1) 바이스테이블 모듈(BSM : BiStable Module)

BSM은 발전소의 가동에 따른 각각의 안전변수에 대한 입력값이 사전에 설정된 제한값을 벗어나는지 입력값과 제한값을

비교하여, 입력값이 제한값을 벗어나는 경우에는 각 변수별로 정지를 위한 신호를 출력한다. BSM의 기능은 정지를 위한 신호의 출력뿐만 아니라 정지를 사전에 경고하기 위한 예비정지 신호 출력도 포함한다. 예비정지를 위한 설정값은 정지를 위한 제한값에 약간의 여유를 고려한 값이다.

(2) 동시논리 모듈(CCM : CoinCidence Module)

CCM은 BSM의 신호 출력결과를 주어진 투표논리에 의하여 신호를 결정하여 주어진 RIM과 EIM에 입력하는 기능을 한다. 예비정지의 경우도 BSM의 신호출력을 RIM과 EIM에 입력하는데 실제정지의 경우와 동일하게 투표논리를 사용한다. 채널의 고장이나 시험을 위하여 특정 채널에 대한 폐쇄기능을 제공한다.

(3) 원자로정지 개시모듈(RIM : Reactor trip Initiation Module)

RIM은 CCM으로부터 정지를 위한 신호를 입력받아 정지를 위한 최종신호를 출력하는 기능을 한다. RIM이 신호를 출력하기 전에 연속적인 4번의 신호가 동일한지 확인하여 같은 경우에 신호를 출력함으로 해서 잡음과 같은 불필요한 신호에 의해 원자로의 정지가 불필요하게 발생하는 것을 방지한다.

(4) 공학적 안전설비 개시모듈(EIM : Engineered safety features Initiation Module)

EIM은 원자로정지로부터 발생하는 통제할 수 없는 심각한 사고에 대비하여 공학적 안전설비(ESF)를 작동시켜 방사능의 누출을 방지하거나 제한하는 기능을 한다. ESF는 긴급 노심냉각설비, 방사능 누출을 차단하는 용기 등으로 이들의 작동은 원자로 정지와 동시에 시작되어야 한다. 따라서 출력은 RIM의 출력과 동일하게 발생되어야 한다. RIM과 같이 EIM도 출력신호를 출력하기 전에 4번의 확인과정을 사용해서 잘못된 공학적 안전설비의 작동을 방지한다.

2.2 디지털 원자로 보호시스템의 구조

디지털 원자로 보호시스템의 입력은 AD 변환기를 통하여 디지털화된 원자로 냉각수 온도, 가압기 압력, 냉각수 유량, 증기발생기 압력 등 12개의 변수값이다. 원자로의 운전 이상은 이들 입력변수값에 반영되어 있어서 보호시스템을 거쳐서 최종적으로 원자로 정지신호 발생기와 공학적 안전설비 작동시스템을 각각 동작시키기 위한 2개의 출력값을 발생시킨다. 따라서 원자로 보호시스템은 입력신호를 처리하여 필요시 출력신호를 발생시키는 변환기능을 한다. 기존의 아날로그 원자로 보호시스템도 아날로그 값을 사용하여 유사한 변환기능을 수행하며 신뢰성을 높이기 위하여 채널 3개에 대하여 투표 구조인 2/3 G 구조를 이루고 있다. 그러나 설계되는 디지털 보호시스템은 디지털기기의 확인되지 않은 신뢰성 문제를 고려하여 이중화된 4개 채널로 구성하였으며 4개의 채널의 모듈들을 스위칭설비를 통해 네트워크로 결합하여 더욱 신뢰성 높은 구조로 구성하였다.

설계되는 디지털 원자로 보호시스템의 구조는 <그림 1>과 같다. 시스템은 입력신호를 출력신호로 변환하기 위하여 기본적으로 BSM, CCM, RIM, EIM의 4종류의 모듈을 사용하며 4개의 채널로 구성된다. 각 채널은 4종류의 모듈이 이중화되어 구성되어 있다. 한편 이중화 되어 있는 각 채널에서 왼쪽에 위치한 모듈을 묶어 하나로 하고 또 오른쪽에 위치한 모듈을 묶어서 하나로 하여 2개의 트레인(train)을 이루고 있다. 이 2개의 트레인은 독립적으로 신호를 처리하도록 설계되었다. 각 채널에서 BSM-CCM-RIM의 구성은 원자로 정지를 위한 신호를 처리하고, BSM-CCM-EIM의 구성은 공학적 안전설비를 작동시키기 위한 신호를 처리한다. BSM과 CCM은 RIM과 EIM에 연결되어 채널이 구성되어 있다. 그림에서 표시된 BSM_A1은 BSM이 1번 채널의 트레인 A의 구성에 사용됨을 뜻하고, BSM_B1은 BSM이 1번 채널의 B 트레인을 구성함을 뜻한다. 따라서 BSM은 4개 채널에 2개의 트레인을 구성하기 위하여 사용되므로 시스템은 총 8개의 BSM이 사용되고 있다. CCM, RIM, EIM에 대하여도 마찬가지로 이들이 사용된 트레인과 채널을 표시하였으며 각 모듈들이 8개씩 사용되고 있다. 따라서 보호시스템은 4종류의 모듈이 각각 8개씩 총 32개 모듈이 사용되고 있다.

보호시스템의 작동에 대하여 살펴보면 각 BSM은 디지털화된 신호를 받아 설정값과 비교하여 원자로의 이상유무에 대한 판단신호를 동일 트레인의 4개 채널에 출력한다. 각 CCM은 BSM에서의 판단신호에 대하여 폐쇄를 가진 4중 2투표구조에 의한 신호를 동일 채널 동일 트레인의 RIM과 EIM에 입력한다. 폐쇄를 가진 4중 2투표구조란 다음과 같다. A 트레인의 4개 채널의 BSM 판단신호에 대하여 1개 채널에서 BSM의 출력이상이 발생하면 투표에 따라 이 채널을 폐쇄하여 3개 채널의 BSM만 작동한다. 이 때 다시 1개의 채널에서 BSM의 출력에 이상이 발생하면 투표에 따라 이 채널을 폐쇄하여 2개의 BSM으로 작동한다. 그러나 만약 2개의 BSM이 작동 중에 서로의 출력이 상이하면 어떤 채널의 BSM에 고장이 발생했는지 판단하기 불가능하므로 보호시스템의 A트레인이 고장으로 간주되는 것이다. CCM에 대하여 이와 같은 폐쇄를 가진 2/4 G 투표구조의 신호를 사용한 것은 BSM에 의해 나타나는 고장의 영향을 완화하고 동일 트레인의 RIM과 EIM에 모두 동일한 입력신호를 제공하기 위한 것이다. 여기서 같은 트레인에 투표기능을 하는 CCM을 4개의 채널에 맞추어 중복 사용한 것은 투표기능의 신뢰성을 높이기 위한 것이다.

각 채널 내에서 2개의 RIM은 동일 트레인의 CCM으로부터 변수별 원자로정지신호를 입력 받아 원자로정지신호를 생성하는데 다른 트레인의 RIM의 신호와 더불어 병렬구조로 하여 최종 원자로정지신호를 출력한다. 이들 신호는 채널별로 발생되는데 CCM과 같이 폐쇄를 가진 2/4 G 투표구조의 신호에 의하여 원자로정지신호발생기에 입력신호를 제공한다. 이 때 폐쇄를 가진 2/4 G 투표구조의 투표기능장치는 분석하고자 하는

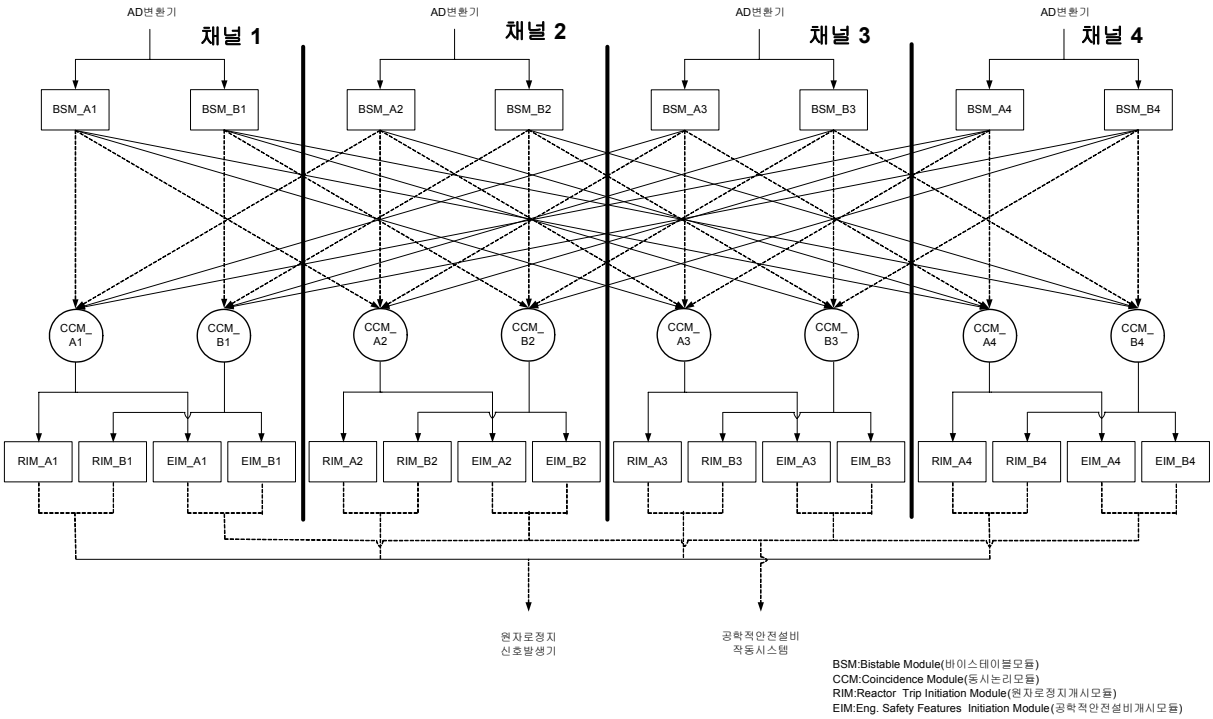

그림 1. 디지털 원자로 보호시스템의 블록 그림

원자로 보호시스템에 포함시키지 않는다. 또한 EIM에 대하여도 RIM과 동일한 논리로 공학적 안전설비 작동시스템에 신호를 출력한다. 이는 원자로가 정지되면 공학적 안전설비(ESF)도 동시에 작동하여 사고의 결과를 완화시키고 방사능 물질의 누출을 제한하는 기능을 하여야 하기 때문이다. 지금까지 설명한 구조에서 모든 모듈들의 연결은 스위칭설비를 통하여 네트워크로 연결된다.

3. 결함나무 모형화

디지털 원자로 보호시스템의 기능은 원자로의 가동과 관련한 여러 입력변수값에 기초하여 원자로 가동에 이상이 발생했을 때 이를 감지하여 착오 없이 원자로 정지신호 발생기에 정지신호와 공학적 안전설비 작동시스템에 작동신호를 전달하여 원자로의 가동을 중단시킴과 동시에 공학적 안전설비를 작동시킨다. 따라서 원자로 보호시스템의 고장은 AD 변환기를 통한 원자로 작동 변수의 이상값에 대하여 이를 변환하여 원자로 정지신호발생기와 공학적 안전설비 작동시스템을 작동시키는 신호를 발생시키지 못하거나, 작동 변수에 이상값이 존재하지 않지만 원자로 정지신호 발생기에 정지신호와 공학적 안전설비 작동시스템에 작동신호를 전달하여 원자로의 가동을 중단시킴과 동시에 공학적안전설비를 작동시키는 착오이다. 그러나 모듈들은 주기적 중복 검사(cyclical redundancy checking), 램검사(RAM checking) 등의 검사와 더불어 RIM과 EIM은 출력신호를 4번 확인하는 과정을 거치므로 보호시스템의 착오는 무시할 수 있다. 따라서 작성할 결함나무모형의 정상사상은 발전소의 가동 시 이상이 발생했다는 가정 하에서 보호시스템을 구성하는 모듈의 고장으로 원자로 정지신호 발생기 또는 공학적 안전설비 작동시스템에 작동신호가 전달되지 못하는 것으로 정의한다. 디지털 원자로 보호시스템은 소프트웨어도 포함되어 있지만 하드웨어 측면에서만 보호시스템의 정상사상에 대한 안전성을 평가하려 한다.

<그림 2-a>, <그림 2-b>, <그림 2-c>의 3개의 그림은 작성된 동적 결함나무모형을 나타내고 있다. 스위칭설비의 고장은 촉발사상으로 통신에 문제를 일으켜 모든 모듈의 기능을 중지시킨다. 한편 <그림 2-b>에서 R1은 원자로 정지신호발생기에 신호 미전달을 출력하는 3/4 F의 게이트에 하나의 입력이다. R2는 R1과 같은 모양이지만 R1에서 기본사상인 CCM_A1고장, CCM_B1고장, RIM_A1고장, RIM_B1고장이 기본사상인 CCM_A2고장, CCM_B2고장, RIM_A2고장, RIM_B2고장으로 구성된 것이다. R3, R4도 유사하게 채널3과 채널4의 CCM과 RIM의 고장을 나타낸다. 또한 <그림 2-c>의 E1은 공학적 안전설비 작동시스템에 신호 미전달을 출력하는 3/4 F의 게이트에 하나의 입력이다. E2는 E1과 같은 모양이지만 E1에서 기본사상인 CCM_A1고장, CCM_B1고장, EIM_A1고장, EIM_B1고장이 CCM_A2고장, CCM_B2고장, EIM_A2고장, EIM_B2고장으로 되어진 것이다. E3, E4도 유사하게 주어진 것이다.

원자로 정지신호발생기에 신호 미전달을 살펴보면 3/4 F의 입력이 주어지는데 이것은 반대로 원자로 정지신호발생기에 신호를 전달하기 위해서는 2/4 G의 입력이 주어져야 하기 때문이다. 공학적 안전설비 작동시스템에 신호 미전달의 경우도

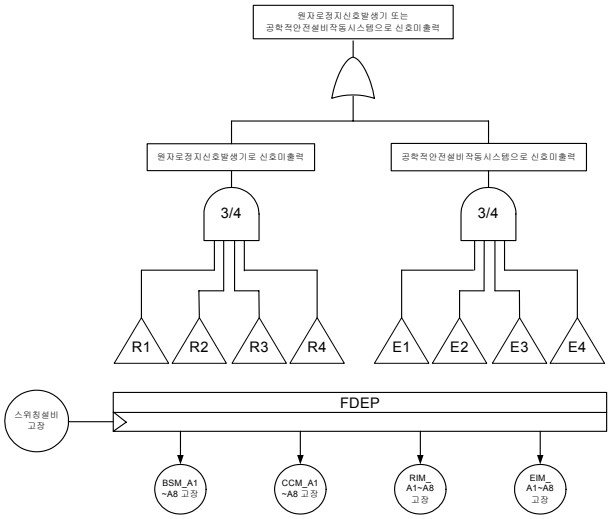

그림 2-a. 원자로 보호시스템 고장에 대한 결함나무모형

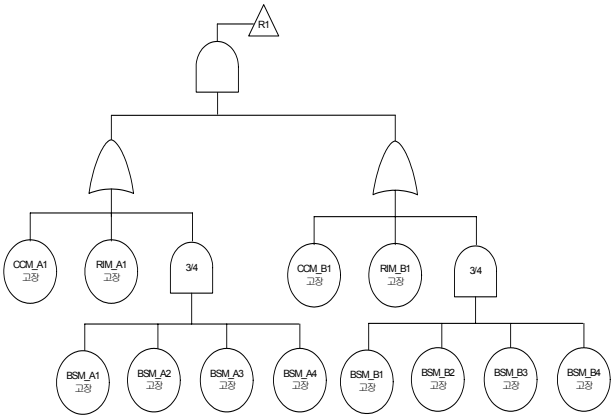

그림 2-b. <그림 2-a>의 전달입력 R1

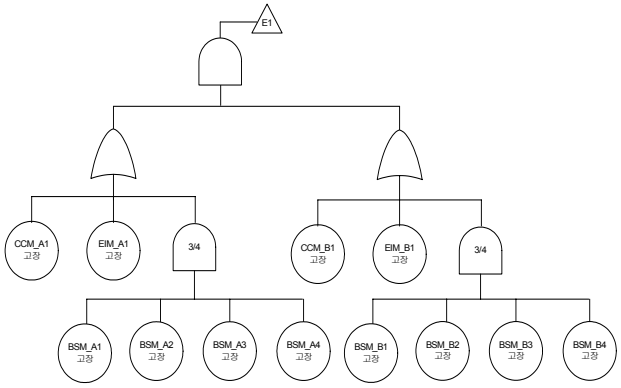

그림 2-c. <그림 2-a>의 전달입력 E1

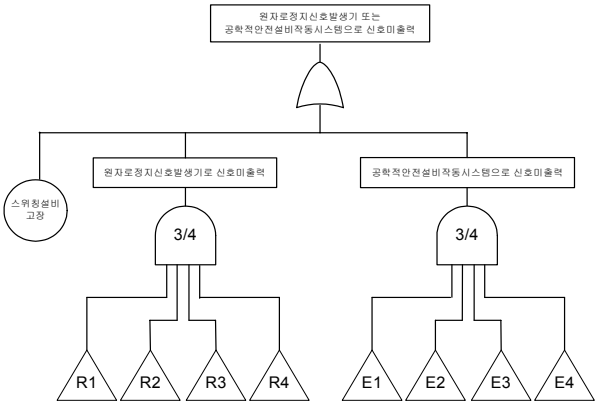

그림 3. 기능적 종속 게이트 없이 표현된 결함나무모형

마찬가지이다. 한편 R1을 살펴보면 BSM에 대하여도 각 트레인에 대하여 3/4 F의 BSM 고장은 반대로 각 트레인에 대하여 2/4 G의 BSM 정상이 되어야 하기 때문이다. R2, R3, R4, E1, E2, E3, E4의 경우도 같다.

완성된 <그림 2-a>의 결함나무모형은 기능적 종속을 나타내는 동적게이트를 포함하고 반복되는 기본사상들을 가지고 있다. 그러나 기능적 종속 게이트를 각 기본사상과 촉발사건이 입력되는 OR 게이트로 대체하면 동적게이트가 없는 결함나무모형으로 표현된다(Vesely, 2002). 더욱이 스위칭설비의 고장은 정상사상을 발생시키므로 스위칭설비의 고장은 정상사상을 발생시키는 OR 게이트에 직접 입력으로 주어지는 결함나무모형으로 <그림 3>과 같이 표현된다.

4. 디지털 원자로 보호시스템의 안전성 분석

4.1 정성적 분석

Dutuit *et al.*(1996)의 선형시간 알고리즘에 의하면 작성된 결함나무모형은 부나무로 나누어지지 않는 하나의 결함나무이다. Relex 소프트웨어를 이용하여 계산한 정상사상에 대한 최소컷집합은 1053개이다. <표 1>은 계산된 최소컷집합을 나타낸 것이다. 스위칭설비 S의 고장을 제외한 1052개의 최소컷집합은 모두 크기가 6이다. 즉 32개의 모듈 중에 특별한 6개 모듈의 고장으로 정상사상이 발생되고 있다. 한편 원자로 정지신호 미출력과 공학적 안전설비 작동신호 미출력에 대한 최소컷집합은 각각 576개이고 따라서 576+576-1052 = 100개의 최소컷집합은 BSM과 CCM 만의 특별한 6개의 고장으로 원자로 정지신호 미출력과 공학적 안전설비 작동신호 미출력이 동시에 발생하는 최소컷집합들이다. 즉 <표 1>의 번호 1049의 BSM_B1고장, BSM_B3고장, BSM_B4고장, CCM_A2고장, CCM_A3고장, CCM_A4고장은 이들 100개의 최소컷집합 중에 하나로 원자로 정지신호 미출력과 공학적 안전설비 작동신호 미출력을 동시에 발생시키는 최소컷집합이다.

<그림 1>의 채널 1과 트레인A에 속하는 BSM_A1, CCM_A1, RIM_A1, EIM_A1의 고장인 기본사상들의 구조중요도를 나타낸 것이 <표 2>이다. Birnbaum의 구조중요도(Barlow *et al.*,1975)는 기본사상의 발생확률과 무관하고 단지 구조상에서 기본사

표 1. 정상사상에 대한 최소컷집합

번호	최소컷집합
1	S고장
2	RIM_A1고장, RIM_B1고장, RIM_A2고장, RIM_B2고장, RIM_A3고장, RIM_B3고장
3	RIM_A1고장, RIM_B1고장, RIM_A2고장, RIM_B2고장, RIM_A4고장, RIM_B4고장
4	RIM_A1고장, RIM_B1고장, RIM_A3고장, RIM_B3고장, RIM_A4고장, RIM_B4고장
5	RIM_A2고장, RIM_B2고장, RIM_A3고장, RIM_B3고장, RIM_A4고장, RIM_B4고장
6	RIM_A1고장, RIM_B1고장, RIM_A2고장, RIM_B2고장, RIM_A3고장, CCM_B3고장
7	RIM_A1고장, RIM_B1고장, CCM_A2고장, RIM_B2고장, RIM_A3고장, RIM_B3고장
8	RIM_A1고장, CCM_B1고장, RIM_A2고장, RIM_B2고장, RIM_A3고장, RIM_B3고장
9	CCM_A1고장, RIM_B1고장, RIM_A2고장, RIM_B2고장, RIM_A3고장, RIM_B3고장
10	RIM_A1고장, RIM_B1고장, RIM_A2고장, CCM_B2고장, RIM_A3고장, RIM_B3고장
11	RIM_A1고장, RIM_B1고장, RIM_A2고장, RIM_B2고장, CCM_A3고장, RIM_B3고장
⋮	⋮
1049	BSM_B1고장, BSM_B3고장, BSM_B4고장, CCM_A2고장, CCM_A3고장, CCM_A4고장
1050	CCM_A4고장, CCM_B4고장, EIM_A2고장, EIM_B2고장, EIM_A3고장, EIM_B3고장
1051	CCM_A4고장, EIM_A2고장, EIM_B2고장, EIM_A3고장, EIM_B3고장, EIM_B4고장
1052	CCM_B2고장, CCM_A4고장, EIM_A2고장, EIM_A3고장, EIM_B3고장, EIM_B4고장
1053	BSM_B2고장, BSM_B3고장, BSM_B4고장, CCM_A3고장, EIM_A2고장, EIM_A4고장

상의 중요성에 대한 측도로 기본사상 A에 대하여 다음 식 (1)과 같이 계산된다.

$$I(A) = 2^{-(n-1)} \times n(A) \quad (1)$$

여기서 n은 결함나무모형에서 기본사상의 개수이며 $n(A)$는 기본사상 A의 임계컷집합의 개수이다. 다른 채널과 트레인에도 동일한 모듈이 사용되므로 동일한 모듈들은 채널과 트레인에 무관하게 모두 동일한 구조중요도를 가진다. <표 2>의 구조중요도를 살펴보면 스위칭설비 S의 고장은 모듈들의 네트워킹을 중지시켜 정상사상의 발생에 제일 중요하고 CCM 고장, BSM고장이 다음으로 중요하며, RIM과 EIM의 고장은 같은 중요도를 가지며 가장 중요도가 낮다.

표 2. 구조중요도

기본사상	구조중요도
BSM_A1고장	0.043380
CCM_A1고장	0.051583
RIM_A1고장	0.032068
EIM_A1고장	0.032068
S고장	0.238451

한편 <그림 3>의 결함나무에 대하여 쌍대나무를 작성하여 최소컷집합을 구하여 얻어진 <그림 3>의 결함나무에 대한 최소패스집합은 18576개로 주어졌으며 모든 집합은 스위칭설비 S의 작동을 포함하고 있으며 크기에 따른 집합의 개수는 <표 3>과 같다. 최소컷집합과 달리 개수도 많으며 크기도 9부터 13까지 다양하다. 이는 결함나무의 분석에서 최소컷집합을 이용하는 이유이기도 하다.

표 3. 최소패스집합의 크기와 개수

크기	개수
9	72
10	222
11	504
12	6912
13	10800

4.2 정량적 분석

정량적 분석을 위해서 기본사상인 모듈의 고장에 대하여 고장률을 구하여야 한다. 각 모듈은 기능요건, 설계요건, 연계요건이 규제 기관에서 요구하는 요건에 따라 설계되었다. 모듈의 고장률은 기본적 구성부품이 지수분포를 따르며 직렬구조라는 가정 하에 MIL-HDBK-217F에 기초하여 계산된다. 그러나 내결함성을 가지는 모듈의 중요한 구성품 DSP 카드에 대하여는 마코프과정 모형을 이용하여 구하여진 신뢰도를 회귀분석을 통하여 일정한 고장률로 예측하고자 한다.

(1) 구성모듈의 고장률 분석

모듈들은 모두 DSP 카드를 포함하고 있다. 그리고 DSP 카드는 와치독(watchdog) 타이머를 이용하는 감시, 자가진단, 복구기능을 가지는 내결함성 설계를 채택하고 있다. MIL-HDBK-217F에서의 부품-스트레스 방법은 시스템을 구성하는 부품이 직렬구조라는 가정 하에서 시스템의 고장률을 예측한다. 따라서 내결함성 설계를 가지는 DSP 카드에 대하여 고장률을 제대로 예측하지 못한다. Lee *et al.*(2008)은 마코프과정 모형을 이용하여 내결함성을 갖는 DSP 카드에 대하여 시간 t에서의 신뢰도를 다음 식 (2)와 같이 예측하였다.

$$R(t) = 1.227e^{-5.327\times10^{-6}t} - 0.227e^{-6.12\times10^{-6}t} \quad (2)$$

식 (2)를 살펴보면 DSP 카드의 고장은 엄밀하게 지수분포를 따르지 않는다. 그러나 Drenick의 정리(Park, 1999)에 의하여 지수분포로 가정할 수 있지만 정량적으로 고장이 지수분포를 따르는지 살펴본다. 전자기기의 수명은 보통 길어야 10여년 정도 이므로 식 (2)에 대하여 0부터 100,000시간(약 11년)까지 1000시간마다 계산된 식 (2)의 신뢰도값의 대수를 반응변수로 하고 시간을 예측변수로 하여 Minitab 소프트웨어를 이용하여 절편이 없는 선형회귀분석을 행하여 얻어진 회귀식은 $\ln R(t) = -5.15339\times10^{-6}t$이다. 따라서 고장률의 추정값은 5.15339×10^{-6}/시간이다. 그러나 잔차에 대한 분석에서 모형의 선형성, 오차의 정규성, 등분산성, 독립성 등에서 약간의 문제를 보인다. 그러나 다음의 식 (3)과 같이 계산된 고장률 추정치의 오차백분율은 0.2%를 넘지 않는다.

$$\text{고장률 추정치의 오차백분율} = \frac{|\ln\widehat{R(t)} - \ln R(t)|}{\ln R(t)} \times 100 \quad (3)$$

따라서 DSP 카드의 고장은 근사적으로 지수분포를 따른다고 가정하고 고장률을 5.15339×10^{-6}/시간으로 신뢰도 함수를 $R(t) = e^{-5.15339\times10^{-6}t}$로 추정한다.

각 모듈은 또한 네트워크 인터페이스 카드(NIC)를 포함하고 있는데 이를 MIL-HDBK-217F의 부품-스트레스 방법에 의하여 계산한 고장률은 $\lambda = 3.84341\times10^{-7}$/시간이다. 디지털 출력장치 DO의 고장률은 $\lambda = 4.04941\times10^{-6}$/시간으로 계산되었다. <표 4>는 각 모듈의 추정된 고장률을 보여준다. 모든 모듈은 NIC를 하나씩 갖고 있지만 BSM, CCM, EIM은 기능적으로 NIC로 입력받아 DSP 카드에서 처리 후 NIC로 출력을 하므로 신뢰도 구조상 고장률 계산에서 NIC의 고장률이 2배로 계산되었다. 한편 각 모듈의 NIC는 스위칭설비를 통해 네트워크로 연결되어 있는데 제작회사에서 제공하는 신뢰성 자료에 의하면 스위칭설비의 고장률은 $\lambda = 1.0\times10^{-7}$/시간으로 알려져 있다.

표 4. 모듈의 구성카드 및 고장률

모듈	구성 카드	고장률(/시간)
BSM	DSP, NIC	5.92207×10^{-6}
CCM	DSP, NIC	5.92207×10^{-6}
EIM	DSP, NIC	5.92207×10^{-6}
RIM	DSP, NIC, DO	9.58714×10^{-6}

(3) 정상사상의 발생확률에 대한 분석

기본사상을 구성하는 모듈의 고장에 대한 발생률(고장률) λ와 임무시간 t가 주어지면 임무시간 동안 기본사상(BE)이 발생할 확률은 다음의 식 (4)로 계산된다.

$$P(BE) = 1 - e^{-\lambda t} \quad (4)$$

따라서 임무시간 동안 정상사상 T의 발생확률은 다음의 식 (5)로 계산된다.

$$P(T) = P(\bigcup_{i=1}^{m} C_i) \approx \sum_{i=1}^{m}\prod_{j=1}^{k_i} P(BE_{ij}) \quad (5)$$

여기서 $C_1, C_2, \cdots, C_m$은 결함나무의 최소컷집합들이고 $C_i = \{BE_{i1}, BE_{i2}, \cdots, BE_{ik_i}\}$이다. 즉 BE_{ij}는 최소컷집합 C_i의 j번째 기본사상이다. 식 (5)의 근사계산은 최소컷집합들이 서로 배반이며 더불어 최소컷집합을 구성하는 기본사상들이 서로 독립이며 낮은 발생확률을 가질 때 성립한다. 일반적으로 근사계산은 결함나무를 구성하는 기본사상의 개수가 많아서 이에 따라 최소컷집합의 수가 상당히 많은 경우에 유용하며 각 기본사상의 발생확률이 0.1보다 작은 경우 계산된 정상사상의 발생확률의 오차는 10% 내에 있다고 한다(Vesely, 2002). 그러나 Relex 소프트웨어를 이용하면 정상사상의 발생확률을 정확히 계산할 수 있다. 또한 크기가 큰 최소컷집합에 대하여 이를 생략하고 정상사상의 발생확률을 근사적으로 계산할 수도 있다.

정상사상의 발생확률을 100,000시간까지 나타낸 것이 <그림 4>이다. 한편 EPRI-URD에 의하면 보호시스템의 신뢰성 목표가 평균고장시간 50년을 요구하고 있다. 이와 같은 신뢰성 목표를 달성하기 위한 정상사상의 발생확률을 같이 나타내었는데 이를 보면 약 45,000시간까지는 정상사상의 발생확률이 신뢰성 목표를 만족하고 있다. <그림 5>는 정상사상의 발생률을 신뢰성 목표의 고장률과 함께 보여주고 있다. 정상사상의 발생률은 시간의 초기에 거의 일정한 발생률을 갖다가 약 10,000시간에서 조금씩 증가를 보이기 시작한다. 현재 안전을 위해서 보호시스템은 18개월(13,140시간)마다 예방정비가 행해지는데 이는 대략 보호시스템의 고장발생률이 증가하기 시작하는 시점과 비슷하다. 18개월(13,140시간)에서의 정상사상의 발생확률은 0.00159525으로 목표값 $1 - e^{-2.283\times10^{-6}\times13140} = 0.029554466$의 5% 정도로 충분히 작다. 마찬가지로 이 때 정상사상 발생률은 2.155×10^{-7}/시간으로 신뢰성목표의 고장률 2.238×10^{-6}/시간의 10% 정도 밖에 되지 않는다.

한편 100,000시간에서 기본사상에 대한 확률중요도를 계산한 것은 <표 5>이다. 다른 채널과 트레인에도 동일한 위치에 동일한 모듈이 사용되므로 동일한 모듈들은 채널과 트레인에 무관하게 모두 확률중요도가 같다. 기본사상을 A라 할 때 위험달성값(risk achivement worth), 위험감소값(risk reduction worth), 임계(criticality), Fussell-Vesely의 중요도는 다음 식 (6)~식 (9)와 같이 계산된다(Vesely *et al*., 1986; Elsayed, 1996).

$$RAW(A) = P(T \mid A=1) - P(T) \quad (6)$$

$$RRW(A) = P(T) - P(T \mid A=0) \quad (7)$$

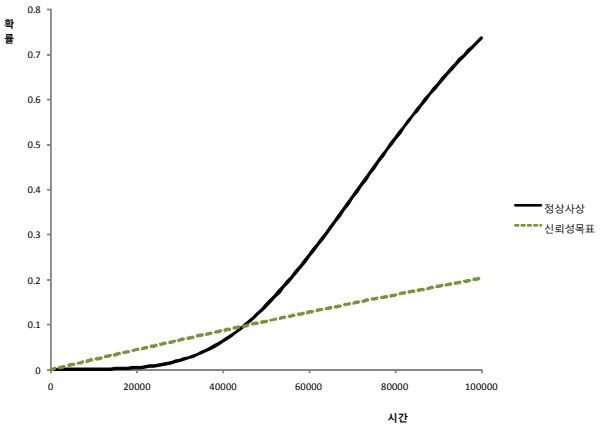

그림 4. 정상사상의 발생확률

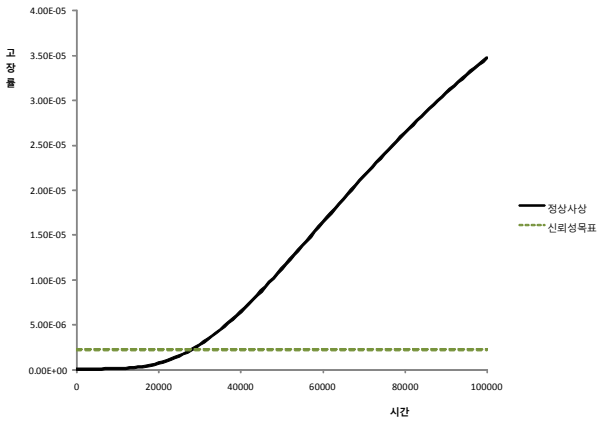

그림 5. 정상사상의 발생률

$$Criticality(A) = P(T \mid A=1) - P(T \mid A=0) \times \frac{P(A)}{P(T)} \tag{8}$$

$$F-V(A) = \frac{P(\bigcup_{A} C_A)}{P(T)} \tag{9}$$

여기서 $P(T)$는 정상사상의 발생확률, $P(A)$는 기본사상 A의 발생확률, $P(T \mid A=0)$은 기본사상 A가 절대 발생하지 않는다는 가정 하에 정상사상의 발생확률, $P(T \mid A=1)$은 반대로 기본사상 A가 반드시 발생한다는 가정 하에 정상사상의 발생확률, $P(\bigcup_{A} C_A)$는 기본사상 A를 포함하는 모든 최소 컷집합의 합집합에 대한 확률이다. <표 5>를 살펴보면 RAW에 의하여 스위칭설비가 현재의 정상사상의 발생확률을 달성하는데 가장 중요하다. 이는 스위칭설비가 상대적으로 낮은 고장률을 가지고 있지만 고장은 모듈사이에 네트워크를 단절시켜 즉시 정상사상을 발생시킴을 나타낸다. RRW에 의하면 현재의 정상사상의 발생확률을 감소시키는데 RIM이 중요함을 알 수 있다. 즉 RIM을 구성하는 디지털 출력 (DO) 카드의 고장률이 DSP 카드보다 훨씬 적은 수의 부품으로 구성되어 있음에도 상대적으로 높은 고장률을 가지는데 이에 대한 개선이 필요함을 알 수 있다. 마찬가지로 임계중요도를 보아도 현재 상대적으로 고장률이 높은 RIM의 개선이 정상사상의 발생확률을 낮추는데 제일 효과적임을 알 수 있다. F-V 중요도는 정상사상을 발생시키는데 잠재적으로 중요한 역할을 하는 것이 CCM임을 나타낸다.

4.3 민감도 분석

제 4.2.1절에서 DSP 카드의 고장시간이 지수분포며 고장률을 5.15339×10^{-6}/시간으로 추정하였다. 이에 따른 민감도를 살펴보기 위하여 $0 \le t \le 100{,}000$에 대하여 식 (2)의 신뢰도 값은 $e^{-5.66873 \times 10^{-6} t} \le$ 식 (2) $\le e^{-4.63805 \times 10^{-6} t}$를 만족한다. 상한과 하한은 추정된 고장률 5.15339×10^{-6}/시간의 10% 만큼의 변화를 고려해서 계산된 신뢰도이다. 따라서 DSP 카드의 고장률에 대한 범위의 하한 4.63805×10^{-6}/시간과 상한 5.66873×10^{-6}/시간에 대하여 정상사상의 발생확률을 나타낸 것이 <그림 6>이다. 100,000시간에서의 정상사상의 발생확률은 하한 0.662456과 상한 0.800244로 추정된 발생확률 0.737407을 기준으로 약 10% 정도 변화를 보인다. 한편 예방정비주기 18개월(13,140시간)에서의 정상사상 발생확률의 하한은 0.00150001, 상한 0.00172608로 추정된 발생확률은 0.00159525를 기준으로 약 80% 변화하여 상당히 크지만 발생확률 자체가 작고 상한의 발생확률도 신뢰성목표의 발생확률보다 충분히 작다.

한편 투표기능을 하는 CCM은 구조중요도 분석에서 스위칭설비 다음으로 중요하고 확률적 중요도 분석에서도 높은 고장률을 가지는 RIM과 더불어 RRW, criticality, F-V에서 높은 중요도를 가지고 있다. 따라서 CCM을 2개, 4개, 8개를 사용하는 경우에 정상사상의 발생확률의 변화를 살펴보자. CCM을 2개 사용하는 경우에 각각은 A와 B 트레인에 하나씩 쓰이고, 각 트레인의 4개 채널에 있는 RIM과 EIM에 신호를 출력하는 경우이다. 4개의 경우는 CCM이 4개의 채널에서 A와 B 트레인에 공통으로 1개가 사용되며, 4개 채널에 있는 RIM과 EIM에 신호를 출

표 5. 확률중요도

기본사상	RAW	RRW	criticality	F-V
BSM고장	0.033258	0.034951	0.041337	0.172874
CCM고장	0.056602	0.045732	0.062018	0.250688
RIM고장	0.040005	0.064340	0.087253	0.241136
EIM고장	0.027422	0.022156	0.030046	0.084751
스위칭설비고장	0.262593	0.002639	0.003579	0.013493

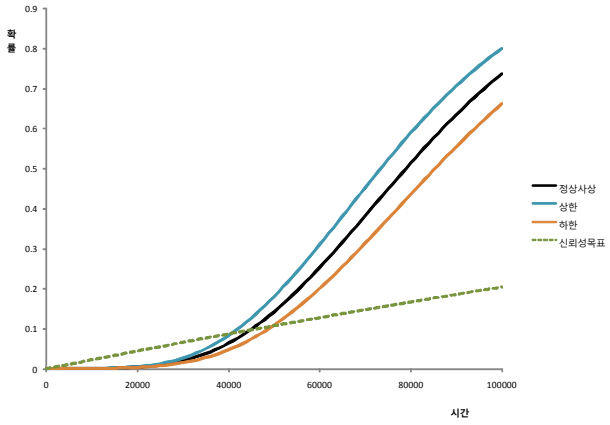

그림 6. DSP 카드의 고장률변화에 대한 민감도

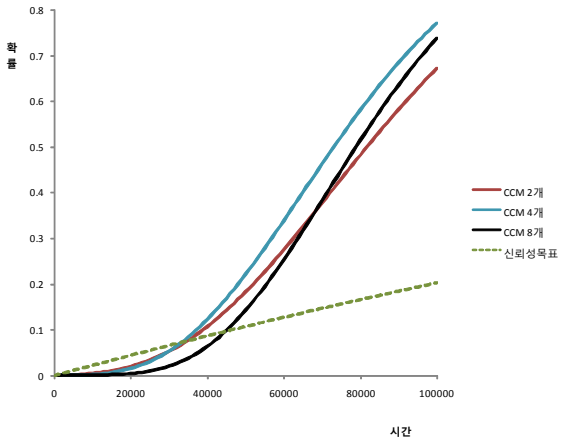

그림 7. CCM 사용 개수에 따른 비교

력하는 경우이다. 2개의 트레인이 독립적으로 신호처리를 해야 한다는 설계요건을 만족하지 않지만 CCM을 제외한 나머지 모듈들은 독립적으로 신호처리를 하는 경우이다. <그림 7>은 정상사상의 발생확률을 나타내고 있다. 68,512시간까지의 구간에서는 8개의 CCM을 사용하는 경우가 정상사상의 발생확률이 가장 낮다. 하지만 이 시점 이후로는 CCM을 2개 사용하는 경우가 정상사상의 발생확률이 더 낮다. 이것은 많은 모듈을 사용하는 경우 시간이 많이 경과하면 고장률이 급격히 증가하기 때문이다. 또한 29,529시간 이후에는 CCM 2개를 사용하는 경우가 CCM 4개를 사용하는 경우보다 우수하다. 현재 보호시스템에 대한 예방정비주기 18개월(13,140시간) 내에서 CCM의 사용 개수가 8개, 4개, 2개 순으로 정상사상의 발생확률이 작고 약 30,000시간 정도 까지는 모두 신뢰성목표의 발생확률을 만족한다.

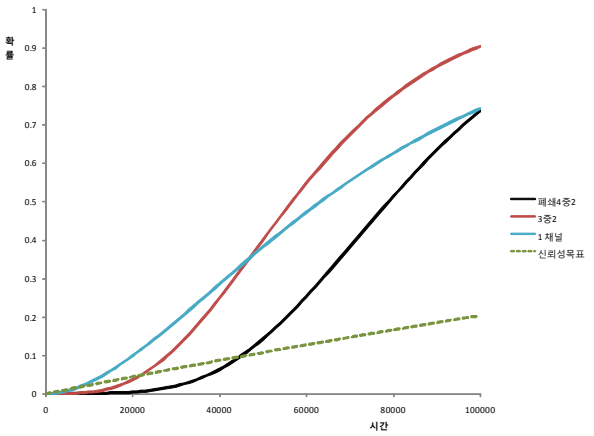

그림 8. 3중 2구조와 폐쇄를 가진 4중 2구조의 비교

또한 폐쇄를 가진 2/4 G 구조의 안전성을 평가하기 위하여 3개의 채널을 사용하는 2/3 G 구조와 비교한 것이 <그림 8>이다. 같이 나타낸 1개 채널만 사용하는 경우는 실제 보호시스템으로 사용될 수 없지만 비교를 위해서 나타내었다. 1개 채널의 경우는 CCM과 스위칭설비가 불필요하여 이것은 계산에서 제외하였다. 한편 Yun *et al.*(2006)은 채널의 중복사용에 대한 근사적인 신뢰도를 알아보고자 A와 B 트레인에 1개씩 CCM을 병렬구조의 1개 채널에 대하여 신뢰도를 분석하였다. <그림 8>을 살펴보면 폐쇄를 가진 4중 2구조가 우수하며 3중 2구조도 18개월(13,140시간) 동안 신뢰성목표에 대한 발생확률을 만족한다. 채택된 폐쇄를 가진 2/4 G 구조는 우주왕복선에서도 채택된 구조로 디지털 기기의 중복 사용으로 내결함성을 가지도록 하는 방법 중의 하나이다(Shooman, 2002). Kang *et al.*(2002)은 PLC를 기반으로 하는 원자로 보호시스템의 선택적 2/4 G 구조의 안전성과 중요한 인자에 대하여 연구하였다. 한편 1개 채널의 경우는 예방정비주기인 18개월(13,140시간) 동안의 신뢰성목표의 발생확률을 만족하지 않는다.

5. 결론 및 향후 연구과제

본 연구에서는 폐쇄를 가진 2/4 G 구조로 내결함성이 우수한 원자력 발전소의 원자로 보호시스템에 대하여 결함나무모형을 이용한 안전성 평가를 수행하였다. 또한 시스템은 디지털 기기의 특징을 반영하여 내결함성을 지닌 DSP 카드 기반의 모듈로 중복 및 이중화되어 구성되어 있다. DSP 카드가 갖는 내결함성의 고려에 대한 추정오차, 투표기능을 하며 채널 폐쇄 기능을 하는 모듈의 사용 개수, 채널수에 따른 대안적 구조 등에 대하여 민감도 분석도 수행하였다. 하드웨어의 고장만을 고려한 한계를 가지고 있지만 평가 결과는 채택된 폐쇄를 가진 2/4 G 구조는 현재 발전소의 예방정비주기인 18개월에 대하여 규제요건을 충분히 만족하여 예방정비주기의 변경도 고려해 볼 수 있을 것 같다.

아울러 후속 연구로는 폐쇄를 가진 구조에서 폐쇄된 채널을 수리하여 안전성을 더욱 증대하는 정비정책, 보호시스템의 수동조작과 관련한 인간-기계 접촉면에서의 인적오류, 보호시스템을 작동시키는 소프트웨어의 고장 및 오류 가능성, 구조상

디지털 시스템이 많은 유사 모듈로 사용하므로 나타나는 공통 원인 고장 등을 고려한 보다 상세한 안전성 평가가 필요하다.

참고문헌

Amari, S., Dill, G., and Howals, E. (2003), A New Approach to Solve Dynamic Fault-Trees, *Proceedings IEEE Annual Reliability and Maintainability Symposium*, 374-379.

Barlow, R. E. and Proschan, F. (1975), *Statistical Theory of Reliability and Life Testing:Reliability Models*, Holt, Rinehart and Winston, Inc.

Bouissou, M. and Bon, J. I. (2003), A New Formalism that Combines Advantages of Fault Trees and Markov Models: Boolean Logic Driven Markov Processes, *Reliability Engineering and System Safety*, **82**(2), 149-163.

Dugan, J. B., Bavuso, S. J., and Boyd, M. A. (1992), Dynamic Fault Tree Models for Fault-Tolerant Computer System, *IEEE Transactions on Reliability*, **41**(3), 363-377.

Dugan, J. B., Sullivan, K. J., and Coppit, D. (2000), Developing a Low-Cost High-Quality Software Tool for Dynamic Fault-Tree Analysis, *IEEE Transactions on Reliability*, **49**(1), 49-59.

Dutuit, Y. and Ranzy, A. (1996), A Linear-Time Algorithm to Find Modules of Fault Trees, *IEEE Transactions on Reliability*, **45**(3), 422-425.

Elsayed, E. A. (1996), *Reliability Engineering*, Addison Wesley Longman, Inc.

Gulati, R. and Dugan, J. B. (1997), A Modular Approach for Analyzing Static and Dynamic Fault Trees, *Reliability and Maintainability Symposium*, 57-63.

Kang, H. K. and Sung, T. (2002), An Analysis of Safety-Critical Digital Systems for Risk-Informed Design, *Reliability engineering and System Safety*, **78**, 307-314.

Koren, I. and Krishna, C. M. (2007), *Fault-Tolerant Systems*, Morgan Kaufmann Publishers.

Lee, S. Y., Jung, J. H., and Kong, M. B. (2008), Reliability Prediction for the DSP Module in the SMART Protection System, *IE Interfaces*, **21**(1), 85-95

MIL-HDBK-217F (1991), *Reliability Prediction of Electronic Equipment*, DoD.

Montani, S. *et al*. (2006), A Tool for Automatically Translating Dynamic Fault Trees into Dynamic Bayesian Networks, *Reliability and Maintainability Symposium*, 434-441.

Park, K. S. (1999), *Reliability and Maintenance Engineering*, Yeongji Moonhwasa.

Reay, K. A. and Andrews, J. D. (2002), A Fault Tree Analysis Strategy Using Binary Decision Diagrams, *Reliability Engineering and System Safety*, **78**, 45-56.

Siewiorek, D. P. and Swarz, R. S. (1992), *Reliable Computer Systems Design and Evaluation*, The Digital Press.

Shooman, M. L. (2002), *Reliability of Computer Systems and Networks*, John Wiely and Sons, Inc.

Vesely, W. E., Davis, T. C., Denning, R. S., and Saltos, N. (1986), *Measures of Risk Importance and Their Applications*, NUREG-3385, Nuclear Regulatory Commission.

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

Yun, W. Y., Jeong, C. H., Kim, S. H., and Lee, S. Y. (2006), Reliability Assesment of SMART Reactor Protection System, *Proceeding of ICAPP 2006*, 6293-6300.

공 명 복

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

이 상 용

울산대학교 공과대학 산업공학과 박사과정
현재 : 삼창기업(주) 제이기술연구소장
관심분야 : 신뢰성공학, 기기내환경 검증, 설비보전, 원전수명관리