

원자력 산업에서의 안전성 및 신뢰도 분석

朴昌奎, 鄭源大

韓國原子力研究所 原子爐 安全評價室

I. 서 론

원자력 산업에서의 안전성 및 신뢰성 분석을 이해하기 위해서는 우선 원자력 산업이 타 산업과 어떤 점에서 유사하며, 어떤 점에서 차이가 나는지 밝혀야 한다. 원자력 산업, 특히 원자력 발전소의 설계, 건설, 운영 및 폐기의 전과정에서의 안전성 분석은 타산업과 달라서 방사능의 방출로 인한 대중에 미치는 영향분석이 첫번째 우선 순위를 가지며, 그 다음이 이러한 조건을 만족시키면서 최대한의 이용률을 보장하는 것이다. 따라서 원자력에서의 신뢰성분석은 그 방법론에서는 타산업과 큰 차이가 없지만, 이용률을 최대화하는 관점보다는 안전성을 극대화하는 측면에서 상당한 차이를 보이고 있다. 원자력 발전소는 발전 원리면에서 타 발전소, 특히 석탄이나 석유를 연소시켜 발전하는 화력발전소와 큰 차이가 없다. 물을 데워서 터빈을 돌려서 발전하는 것은 같은 메카니즘이며, 물을 데우는 방법에서 우라늄이나 플루토늄을 사용하느냐 아니면 석유나 석탄을 사용하느냐의 차이이다. 문제는 발전의 부산물로 생기는 방사능의 외부유출을 어떻게 막느냐 하는데 있다.

방사능의 외부 유출을 막기 위하여 원자력 발전소는 크게 다섯가지의 방호층을 가지고 있다. 즉 핵연료 펠렛이라고 부르는 새끼 손가락의 끝마디 정도 크기의 연쇄 핵반응이 직접 일어나는 연료부분이 있다. 펠렛의 속에서 생성된 방사능은 그 속에서 대부분 갇혀 있게 된다. 이것이 제1차 방호층이다. 이 핵연료 펠렛을 길이가 약 3~4m 정도인 핵연료 봉이 싸고 있고, 이 핵연료 봉은 다시 냉각재인 물속에 잠겨 있다. 핵연료 봉과 냉각재가 제2차 및 제3차의 방사능 방호층을 형성한다. 밀폐된 격납용기가 이 모두를 싸고 있어 제4의 방사능 방호층을 이

루며, 마지막으로 약 1m 두께의 철근 콘크리트로 둘러싸인 격납건물이 있어 만약 제4의 방호층을 뚫고 나온 방사능이 있는 경우, 이를 외부로 유출되지 못하게 한다. 이러한 다섯가지의 방호층을 형성하는 개념이 바로 다중방호개념(defence in depth concept)이다. 다중방호 개념과 함께 원자력 안전을 확보하려는 신뢰도 관점에서의 노력이 중첩개념(redundancy concept)이다. 중첩개념은 위에서 간단하게 설명한 각 방호층을 보호하기 위하여 도입된 개념이다. 즉 각 방호층의 보호를 위하여 2개에서 4개까지의 독립적(independence)이고 다양화(diversity)된 각종 공학적 안전장치(engineered safety features, ES-F)를 설치하는 개념이다. 뿐만 아니라 이런 안전장치들이 설사 이용률을 해치는 한이 있더라도 원자력 발전소를 안전한 상태로 가게 하는 것이 fail-safe 개념이다.

앞에서 지적된 바와 같이 원자력에서의 신뢰도 분석은 이와 같은 원자력 고유의 특성이 유지된 상태에서 행해져 오고 있다. 따라서 신뢰도 분석은 독자적인 분야이기 보다는 원자력 발전소의 종합 안전성 평가의 한 부분으로 수행되어 오고 있다. 원자력 발전소의 안전성을 확보하고 확인하기 위한 방법으로는 전통적으로 결정론적인 안전성분석(deterministic safety analysis) 방법이 사용되어 오고 있는데, 이 방법은 발생가능한 중요사고를 선정하고 이러한 사고가 발생하더라도 원전이 안전하다는 것을 확인하는 방법이다. 이때 설치된 안전계통이 정상적으로 기능을 발휘한다는 가정을 하게 되는데, 이러한 가정은 계통의 다중성 및 다양성 확보로 만족한다는 판단하에 그 타당성을 인정하여 왔다. 그러나, 이러한 가정을 넘는 심각한 사고가 발생하면 어떻게 될 것이며, 그러한 사고가 일어날 가능성은 얼마나 되는지에 대한 의문이 제기되기 시작하였다. 이러한 의문에 해답을 주기 위하여 시도된 방법이 확률론적 안전성분석(probabil-

stic safety assessment:PSA)이다. 확률론적 안전성분석 기법은 1975년 완료된 WASH-1400^[1]에서 처음 이용되었으며, 그후 원자력 산업의 안전성 평가에 널리 이용되어 왔다. 종래의 결정론적 분석 방법에 의해서는 나타나지 않던 원전의 취약점을 파악, 개선할 수 있도록 함으로써 원전 안전성을 제고시키는 역할을 담당하여 왔으며, 이제는 운전/보수 절차의 개선, 설계개선, 운전원 교육, 부지선정, 안전성 목표 설정 등 다양한 분야에 응용되고 있다.

II. 확률론적 안전성 분석

원자력 발전소는 많은 안전장치들을 설치하여 사고발생 가능성을 최대한 줄이며, 사고가 발생하더라도 피해의 확대를 최대한 방지하도록 설계되어 있다. 그러나, 많은 안전계통을 설치하고 다중성 및 다양성 확보로 계통의 신뢰도를 높여도 운전원의 오동작이나 안전계통 또는 부품의 작동 실패가 완벽하게 근절될 수는 없으며, 그 가능성은 매우 작지만 안전계통들의 작동불능으로 노심손상을 초래하는 사고가 발생할 수도 있다. 따라서 노심손상을 일으킬 수 있는 초기사고 요인 및 이에 따른 사고경위를 파악하고 그 발생빈도를 추정하며, 만일 이런 사고가 발생하였을 경우 그에 따른 영향을 분석하여 주변 주민의 재산이나 건강, 환경에 대한 피해정도의 중요성을 결정하

고 이러한 중요도에 의거하여 사고대책은 물론 설계·건설·운영 대책을 마련할 필요가 발생하였다. 이러한 욕구를 충족시키기 위해 알맞은 안전성분석 방법이 확률론적 안전성분석 기법이다.^[2,3,4]

확률론적 안전성분석은 그림 1에서 보여주는 바와 같이 크게 세가지 업무로 구분할 수 있다. 첫번째 업무가 계통신뢰도 분석으로 사고요인별로 노심손상에 이를 수 있는 사고경위들을 파악하고 노심손상 발생빈도를 추정하는 과정으로 이에겐 일반적으로 사건수목(event tree) 분석 및 고장수목(fault tree)분석기법이 이용된다.

두번째 업무가 격납용기분석(containment analysis)으로 사고발생후부터 격납용기로부터의 방사능 방출전까지의 현상을 다루며, 여기에서는 각 사고경위별로 격납용기내의 물리적 현상의 진전과정을 분석함과 동시에 격납용기내에 방출되는 방사성 핵종의 이송과 침전현상등을 다룬다. 또한 사고경위중의 물리적 현상에 대한 격납용기의 건전성 유지 정도를 분석하고 격납용기 파손시의 대기중으로의 방사능 방출량을 평가한다.

세번째 업무는 결말분석(consequence analysis)으로서 사고로 인한 격납용기 파손시 대기중으로 방출되는 방사성핵종의 대기중 이송 및 피폭으로 인한 사고피해를 대중에게 미치는 건강상 효과와 경제적 손실로 평가한다.

앞에서 언급한 세가지 분석결과를 결합하면 원전사고로 인한 피해발생 가능성을 사고요인별 사고경위별로 파악할 수 있게 된다. 확률론적 안전성 분석이라 하면 일반적으로 이 세가지 업무를 통틀어 일컫는다. 그러나 확률론적 안전성 분석을 수행하는 목적에 따라 분석업무를 제

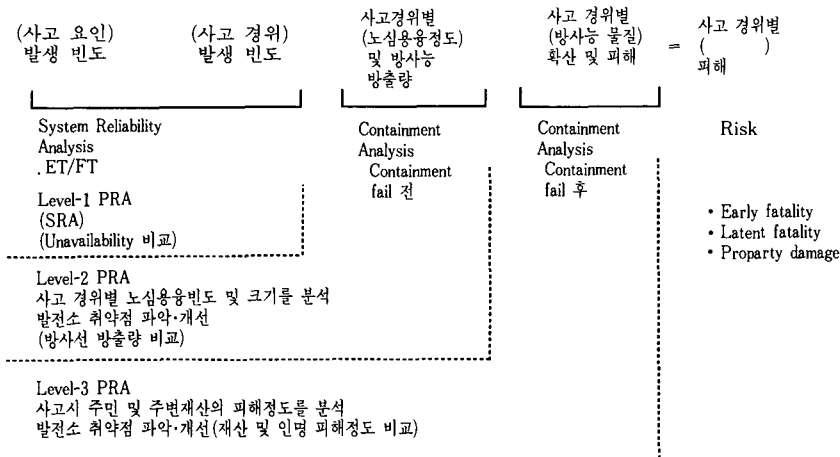


그림 1. 확률론적 안전성분석 업무

한적으로 수행할 수도 있어 계통신뢰도 분석을 통한 노심 손상빈도 도출까지를 level-1 PSA, level-1 PSA와 격납 용기 분석업무까지를 level-2 PSA, 결말분석까지의 전 분석업무를 level-3 PSA라고 구분하여 부르기도 한다. 그림 2에서는 확률론적 안전성 분석의 정보수집 단계에서부터 결말분석에 이르기까지의 수행절차를 보여주고 있다.

Level-2, 3는 주로 현상분석에 대한 내용으로 여기에서는 주로 level-1 확률론적 안전성분석 내용과 분석방법을 정리하고, 격납용기분석, 결말분석은 간단히 소개하는 것으로 하였다.

1. Level-1 확률론적 안전성분석:노심손상경위분석

Level-1 확률론적 안전성분석에서는 원전에서 발생가능한 모든 노심손상 사고경위를 밝혀내고 그 발생빈도를 추정하게 된다. 주요 업무로는 원전에 이상상태를 초래하는 모든 초기사건 유발요인을 파악하고 분류하는 초기사건 분석, 선정된 초기사건들에 대하여 각 초기사건 발생후 일어날 수 있는 모든 사고경위를 밝혀내는 사건수목분석, 여러 안전계통들의 계통신뢰도를 평가하는 계통 고장수목분석, 각종 기기/부품의 고장률과 보수자료 및 인간오류 자료를 추정하고 데이터베이스를 구축하는 자료분석, 불확실성분석 등이 있다.

원자력 발전소의 신뢰성 분석은 크게 두 가지 점에서 타 분야와 차이를 나타내고 있다. 그 하나는 각 기기나 계통의 신뢰성이 높기 때문에 많은 고장 데이터를 수집하

기가 힘어들며 따라서 고전적인 통계 처리가 힘이 든다는 데 있으며, 또 다른 하나는 항상 독립적인 고장의 가정이 성립하지 않는다는데 있다. 즉 공동원인으로 일어나는 계통의 실패율이 대개의 경우 독립적인 고장으로 일어나는 계통의 실패율보다 높다는 것이다. 따라서 희귀사건근사(rare event approximation)가 항상 통하지 않는다는 것이며, 뿐만 아니라 공동원인 고장에 대한 고려가 심각하게 대두된다.

불확실성 분석은 위에서 언급한 대로 각 기기의 신뢰도가 높아서 고장 자료들이 충분치 못하며, 따라서 종래의 통계학적 처리를 하기에는 높은 신뢰성(confidence)을 유지하기 힘이 든다. 이때 고장자료의 처리에 주관적인 공학적 판단(subjective engineering judgement)이 등장하게 되고, 불확실성 분석은 신뢰도 분석 결과의 신뢰성을 높이기 위해 절대적으로 필요하게 되는 것이다.

Level-1 PSA의 가장 중요한 과정인 사고경위분석과 계통신뢰도분석에 대하여 알아보고, 결과에 중요한 영향을 미치는 공동원인고장분석과 인간신뢰도분석에 대해서도 간략히 언급하기로 한다.

1) 사고경위분석

원자력 발전소와 관련된 위험을 정량화하기 위해서는 우선 발생 가능한 모든 사고 시나리오를 밝혀내야 한다. 사고경위분석이란 초기사건 발생후 노심손상을 유발할 수 있는 사건들의 조합을 밝혀내는 작업으로 선정된 초기사건들에 대하여 사건수목을 구성함으로써 중요한 사고경위들을 논리적으로 밝혀내게 된다. 모든 사고경위를 밝혀

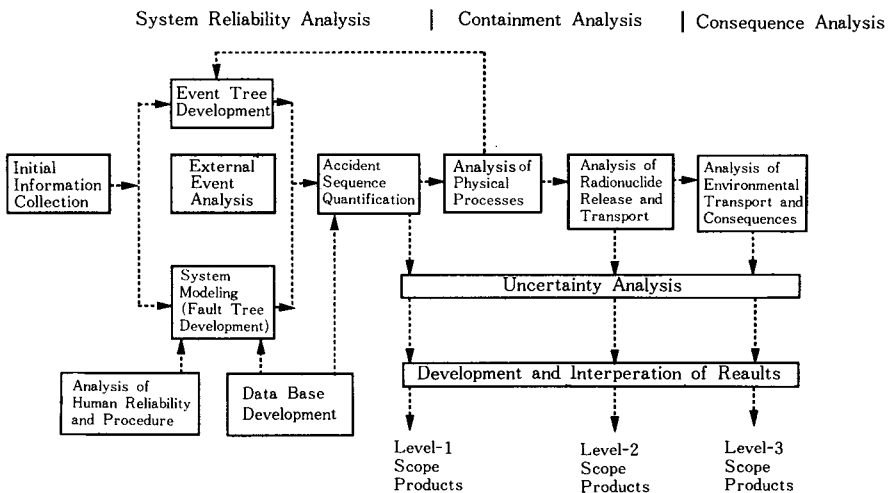


그림 2. 확률론적 안전성분석 절차

내는 작업은 크게 세가지 단계로 구분할 수 있다. 첫째, 발생 가능한 모든 초기사건을 정의하고 사고진행 형태가 유사한 초기사건들을 파악·분류하는 단계. 둘째, 각 사고 경위에 대하여 안전계통들이 성공적으로 기능을 발휘하기 위한 각 계통별 성공기준의 결정. 셋째, 각 초기사건들에 대한 사건수목의 구성으로 되어 있다. 이중 첫째와 둘째 단계는 초기사건분석에서 주로 수행하고 있으며, 사고 경위의 파악은 사건수목분석에서 이루어지나 세 단계가 상호 밀접한 연관관계를 갖고 수행되어야 한다.

초기사건(initiating event)이란 운전중인 발전소를 정상 운전상태에서 이탈시켜 원자로를 정지시키고, 원자로를 안전상태가 되도록 하기 위하여 설치된 안전계통의 자동작동이나 운전원 조치를 유발시키는 최초의 계통고장 또는 인간실수를 말한다. 과거 사고이력이나 사고해석을 통하여 이런 모든 초기사건을 선정하고 초기사건 발생후 발전소 안전계통들의 대응방식이나 사고를 완화시키는 과정이 유사한 초기사건들끼리 묶어 최종적으로 사건수목 구성을 위한 초기사건을 선정하게 된다.

· 사건수목 구성에서는 초기사건 발생후 노심손상을 방지하기 위하여 필요한 안전계통들의 작동 성공, 실패에 따라 수 많은 사고경위가 논리적으로 전개된다. 이들 사고경위중 어떤 사고조합들은 사고를 성공적으로 완화시키는 사고경위가 될 것이며, 어떤 사고경위들은 노심손상을 초래하는 사고조합들이 된다. 이를 판단하기 위하여 때로는 많은 사고해석을 수행하여야 하기도 한다. 또한 모든 가능한 사고경위를 빠짐없이 밝히기 위하여는 초기사건 발생시 이에 관련된 모든 계통들의 정확한 운전특성 및 운전원의 관련작업 파악은 물론 사고로 인해 초래되는 물리적 현상에 의해 생기는 계통들간의 상호연관성 등에 대한 정확한 이해가 필요하다.

사건수목 구성 및 평가를 간단한 예를 통하여 살펴보면 다음과 같다. 초기사건 A가 발생하였을 때, 사고완화 및 복구를 위하여 안전계통 B 및 D의 운전이 성공하든지, 만일 안전계통 B가 실패하는 경우 계통 C 및 D의 운전이 필요하다고 가정하면, 이런 상황에서 발생할 수 있는 관심있는 사고경위는 그림 3에서 보는 바와 같이 5가지가 존재한다. 이중 사고경위 1은 초기사건 A 발생 후 계통 B, D가 모두 정상적으로 작동하여 성공적으로 사고를 완화시킨 경우이며, 사고경위 3은 계통 B는 작동 실패하였지만 다른 안전계통인 C가 성공적으로 작동하고 그 후 계통 D가 정상적으로 운전되어 노심손상을 방지한 사고 경위를 나타낸다. 그러나, 사고경위 2, 4, 5는 계통 B, C, D중 어느 하나나 그 이상이 이용불능이어서 노심손상을 초래하는 경우이다.

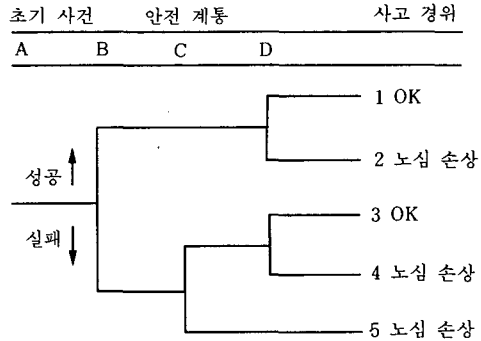


그림 3. 사건수목 구성 예

사고경위 2, 4, 5로 인한 노심손상 발생 빈도를 계산하기 위해서는 우선 초기사건 A의 발생 빈도(frequency)와 계통 B, C, D의 이용불능도(unavailability)를 필요로 한다. 초기사건 발생빈도는 과거 사고이력을 조사하여 추정하며, 계통이 이용불능도는 다음에 언급할 고장수목분석을 통하여 산출하게 된다. 만일 초기사건 A의 발생빈도가 $F(A) = 1.0E-3$ 회/년 이고 계통 D의 이용불능도가 $Pr(D) = 2.0E-3$ 이라면, 사고경위 2로 인한 노심 손상 발생빈도는 $(F) \cdot Pr(C) = 2.0E-6$ 회/년이 된다. 이와같은 방식으로 사고경위 4, 5에 대한 정량화를 수행하면, 초기사건 A로 인한 노심손상 발생 빈도를 추정할 수 있게 된다.

실제 사건수목 구성시에는 고려해야 할 안전계통 및 운전조건들이 훨씬 많아 사건수목은 복잡하게 구성된다. 초기사건에 따라서 다르나 하나의 초기사건에 대하여 많은 경우 20 내지 30 개의 사고경위가 밝혀지는 것도 있으며, 중요하다고 밝혀지는 총 사고경위는 보통 150 내지 250 개 정도가 된다. 위의 예에서는 계통들간의 종속성이 없다고 가정하였으나, 많은 경우 초기사건과 계통간 혹은 계통들간의 종속성(dependency)이 존재하므로 이를 모델링에 적절히 반영하고 평가하는 것이 사고경위분석에서 매우 중요한 일중의 하나가 된다.

2) 계통분석

원자력발전소의 노심손상빈도를 산출하기 위하여는 관련된 모든 계통들의 신뢰도를 분석하여야 한다. 원자력발전소는 여러 종류의 안전계통들이 중복적으로 다중 설계되어 있으며, 계통의 규모가 크고 운전 조건 및 방식이 복잡하게 상호 연관되어 있으므로 계통신뢰도분석은 쉬운 작업이 아니다. 또한 초기사건의 종류에 따라 여러 안전계통들의 기능적 대응이 틀려지게 되며, 동일계통에 대

해서도 사고경위에 따라 성공기준이 달라지기 때문에 모든 사고경위의 발생빈도를 추정하기 위하여는 방대한 양의 계통신뢰도분석이 수행되어야 한다.

원자력발전소의 안전성 평가시 이용되는 계통신뢰도의 평가단위는 계통 이용불능도(system unavailability)로, 임의의 시점에서 안전계통의 작동이 요구되는 사고가 발생하였을 때, 해당 안전계통이 성공적으로 작동하지 못할 확률값으로 표현된다. 안전계통이 성공적으로 작동하지 못한다는 것은 작동요구가 있었을 때 초기작동에 실패하던지, 초기작동에 성공하더라도 주어진 임무시간(mission time)동안 연속작동에 실패하는 것을 의미한다. 계통의 작동불가능 요인으로는 여러가지가 있을 수 있다. 관련계통내의 각종 부품의 고장, 계통내 여러 기기의 작동불능을 초래하는 보조계통(support system)들의-전기, 기기냉각수, 공기냉각, 계기/제어 등 - 기능상실은 물론 시험 및 보수작업과 관련된 인간오류(human error)등이 계통의 이용불능을 유발하게 된다.

계통신뢰도 분석을 위하여 여러 방법이 개발되어 있으나, 원자력 발전소의 계통신뢰도는 일반적으로 고장수목분석을 통하여 평가하고 있다. 고장수목분석은 원자력발전소와 같은 복잡한 계통의 신뢰도를 평가하기에 적합한 방법으로, 계통이 작동불능되는 직접적인 요인들을 연역적 방법을 통하여 파악하고 Boolean 방정식으로 표현한 후, 각 요인들의 발생 확률 자료를 사용하여 계통의 이용불능도를 구하게 된다. 고장수목 구성시에는 관련계통의 부품의 고장은 물론 시험, 보수 및 계통의 운전과 관련된 운전원 실수도 고려하게 되므로 이러한 고장이나 실수에 관련된 신뢰도 자료 즉 부품고장률이나 인간오류 확률의 자료 확보가 중요하게 된다. 또한 고장수목 분석시에는 공통원인 고장이나 타계통과의 연관성 등을 적절히 모델링하는데 주의가 기울여야 한다.

고장수목 분석절차를 간단히 기술하면 다음과 같다.

- (1) 분석대상계통의 성공기준을 토대로 작동실패조건을 결정하여 이를 고장수목의 정점사상(top event)으로 정한다.
- (2) 정점사상이 주어지면 이러한 정점사상이 일어날 수 있는 직접적인 요인을 연역적 방법에 의하여 파악하고 AND 또는 OR gate로 표시한다.
- (3) 정점사상이 일어날 요인파악은 모든 요인들이 부품의 기계적 고장이나 인간오류 등과 같은 기본사건(basic event)으로 표현될 때까지 계속한다.
- (4) 고장수목이 구성된 후에는 이를 Boolean 방정식으로 표시한다.

(5) Boolean 방정식을 풀고 정리하여 정점사상에 이르기 위한 최소단절집합(minimal cut set)을 결정한다.

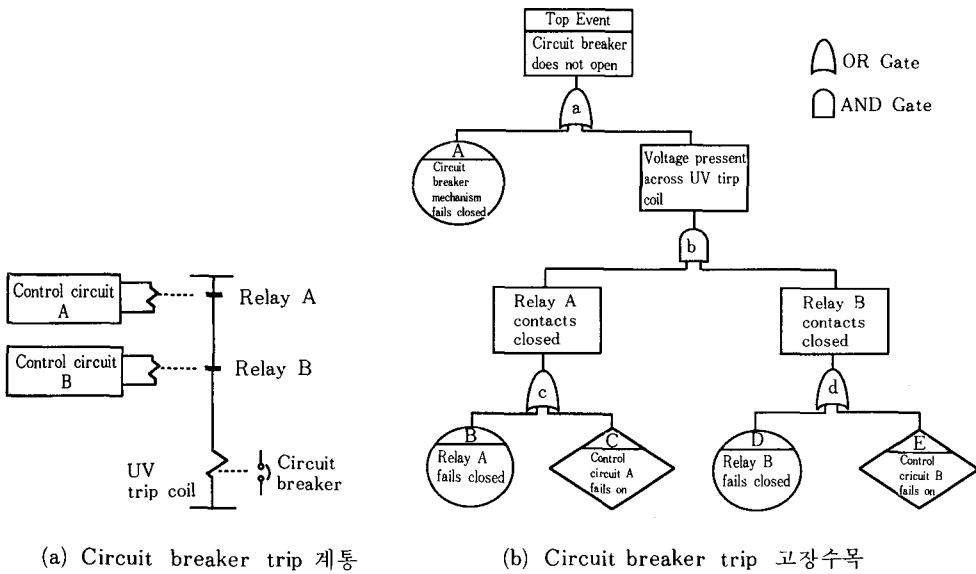
(6) 기본사건들의 확률자료를 이용하여 최소단절집합들의 이용불능도(unavailability)를 계산하고, 정점사상에 대한 모든 최소단절집합들의 이용불능도를 더하여 계통의 이용불능도를 구한다.

고장수목분석을 이해하기 쉽게 하기 위하여 그림 4(a)와 같은 구조를 갖는 circuit breaker의 trip 고장을 살펴보기로 한다. Circuit breaker trip 실패는 “circuit breaker가 열리지 않는다”고 표시할 수 있으며 이를 이 고장수목의 정점사상으로 잡는다. 이 정점사상을 유발시킬 요인들을 연역적으로 파악해 보면, circuit breaker가 열리지 않는 경우는 circuit breaker 자체가 닫혀 있는 상태로 고장이 났거나 UV trip coil에 전류가 흐르는 경우로 표시할 수 있다. 다음에 UV trip coil에 전류가 흐르는 경우는 다시 relay A와 B가 동시에 닫혀 있는 것으로 볼 수 있다. 다시 relay A와 B가 닫혀 있는 경우는 relay 자체 고장으로 인한 고장과 control circuit의 고장에 따른 작동으로 인한 경우로 파악할 수 있다.

이런 논리전개를 고장수목으로 표현하면 그림 4(b)와 같다. 고장수목에서 사용된 기호를 간략히 설명하면, 각 사건에 대한 설명은 직사각형으로, 기본사건은 원으로, 미개발 사건은 마름모로 표현되며, 요인이 되는 하부사건들이 동시에 발생하여야 상부사건이 일어나는 경우에는 AND gate를, 하부사건들중 어느 하나만 발생하여도 상부사건이 일어나는 경우에는 OR gate를 사용하여 정점사상에 대한 고장수목을 구성한다.

그림 4(b)에서 보는데로 gate는 영문소문자로 기본사건은 영문대문자로 표시하였을 때, 이를 이용하여 정점사상 a를 표시하면, $a = A + b = A + cd = A + (B + C)(D + E)$ 와 같이 되며 Boolean 대수를 이용하여 정리하면, $a = A + BD + BE + CD + CE$ 로 표시된다. 이로부터 정점사상 a가 발생하기 위한 단절집합 A, BD, BE, CD, CE가 구해지며, 여기서는 이들 모두가 정점사상 a의 최소단절집합(minimal cut set)이 된다.

만일 각 기본사건들의 발생확률이 $Pr(A) = 0.001$, $Pr(B) = Pr(C) = Pr(D) = Pr(E) = 0.02$ 와 같이 주어졌다면, $Pr(a) = 0.001 + 0.02 \times 0.02 + 0.02 \times 0.02 + 0.02 \times 0.02 = 0.0022$ 로 되어 정점사상 a의 발생확률, 즉 circuit breaker trip 계통의 이용불능도는 0.0022가 된다. 앞의 정점사상 a의 이용불능도 계산시에는 회귀사건근사, 즉 $P(A \cup B) \approx P(A) + P(B)$, 기법이 사용되었음을 언급하여 둔다.



(a) Circuit breaker trip 계통

(b) Circuit breaker trip 고장수목

그림 4.

3) 인간신뢰도분석(human reliability analysis)

이제까지 경험한 사고이력이나 기 수행된 PSA 결과를 통하여 인간행위는 원전 안전성에 중요한 영향을 미치는 인자중의 하나로 밝혀지고 있다. 원전 안전성에 영향을 주는 인간행위로는 시험 및 보수작업, 계기교정 및 이상 상태 발생시 복구조치 등이 있으며, PSA 수행시 이들 인간행위들은 계통의 고장수목이나 사고경위를 밝혀내는 사건수목에서 모델링된다. 인간신뢰도분석은 모든 사고경위 도출시 발생가능한 모든 인간오류를 정의하고 모델링하며 정량화하는 작업으로 PSA 업무의 중요 수행분야중의 하나이다.

인간신뢰도 분석 수행은 노심손상을 유발할 수 있는 모든 사고경위와 관련된 인간오류를 밝혀내고 정량화하는 작업이므로 level 1 PSA의 다른 업무와 밀접한 상호관계를 갖고 반복적으로 수행되어야 한다. 대표적인 인간신뢰도 분석 절차로는 THERP(technique of human error rate prediction)^[5]와 SHARP(systematic human action reliability procedure)^[6]가 있으며, 두 절차 모두 유사한 수행절차를 포함하고 있다.

SHARP 방식에 의한 HRA 수행절차는 다음과 같다.

- 인간오류 정의(definition): 인간오류의 정의는 원전 운전 및 보수와 관련되어 발생가능한 모든 인간오류를 밝혀내고 고장수목이나 사건수목에 모델링하는 단계이다. 이 단계에서는 운전/보수절차서 및 현장 요원과의 정보교환을 통하여 발전소에서 실제로 발

생가능한 모든 인간오류를 찾아내고 정의하여야 한다. PSA 수행시 정의된 인간오류들은 관련 작업의 특성이나 관련 행위 유형의 유사성에 따라 몇 가지로 분류가 가능하다. 정상운전시 일상적인 시험이나 보수작업과 관련한 인간오류와 이상상태 발생시 복구운전과 관련된 인간오류로 크게 구분할 수 있는데, 이들 인간오류와 관련된 인간행위의 특성 및 영향 인자는 많은 차이가 존재하며 따라서 분석 방법도 달라지게 된다.

- 선별(screening): Screening 단계는 상세분석이 필요한 인간오류를 선별하는 과정이다. Definition 단계에서 정의한 모든 인간오류들이 전부 노심손상에 큰 영향을 미치는 것은 아니며, 따라서 모델링된 모든 인간오류에 보수적으로 큰 확률값을 지정하여 정량화한 후 계통의 이용불능이나 노심손상에 큰 영향을 미치는 것은 보수적인 값을 그대로 사용하고, 큰 영향을 미치는 인간오류는 선별하여 상세한 분석을 수행하게 된다.
- 분석(breakdown): 분석단계는 선별된 인간오류에 대하여 상세분석에 필요한 모든 정보를 수집하는 단계로 인간오류 분석을 위하여 선택한 정량화 모델에서 필요로 하는 입력자료를 수집하고 시험/보수 절차서 및 비상운전절차서를 검토하여 대상작업 수행에 필요한 세부행위, 작업의 난이도, 대상기기 및 장비의 설계특징, 작업환경, 시간정보, 운전원 숙련도

및 심리상태 등 분석에 필요한 모든 상세 정보를 수집하게 된다.

- 인간오류 표현(representation): 이 단계는 기존의 개발된 분석모델중 적절한 모델을 사용하여 인간오류를 표현하고 모델링하는 과정으로, THERP, OAT(operator action tree), TRC(time reliability correlation), HCR(human cognitive reliability) model, SLIM(success likelihood index method), confusion matrix 등의 모델이 사용되고 있다. 인간오류는 크게 인식/진단과정에서 발생하는 오류와 반응단계에서 발생하는 오류로 구분되며 각 오류의 평가에 알맞은 분석모델을 이용하여 표현하고 모델링 한다. 인식/진단단계에서 발생하는 인간오류는 대상작업의 난이도, 작업허용시간, 절차서의 수준 및 숙련도 등에 큰 영향을 받으며, 이 유형의 인간오류 평가에는 TRC 및 HCR 모델이 널리 이용되고 있다. 반응단계에서 발생하는 인간오류는 구체적인 동작 수행과정에서 발생하는 오류로, 인간의 행위를 단위동작으로 분해한 후 각 단위동작에 대한 오류 가능성을 평가하게 된다. 이 유형의 인간오류 평가에는 THERP 방법이 널리 사용되고 있다.

- 정량화(quantification): 정량화단계에서는 선택한 모델 및 기용자료를 사용하여 오류 확률값을 산출하게 된다. 단위 인간행위에 대한 오류 확률값은 HRA Handbook^[7] 자료가 널리 이용되고 있으며, 최근에는 발전소 모의운전설비를 이용한 모의실험을 통하여 구체적인 사고상황에 대한 인간오류 자료를 모으고, 이를 분석하여 정량화에 이용하고 있다.

4) 공통원인고장분석(common cause failure analysis)

최근 확률론적 안전성평가의 계산결과인 노심손상빈도에 큰 영향을 미치는 것으로 나타난 주요 인자의 하나로서 공통원인고장이 부각되고 있다. 공통원인고장이란, 공통된 원인에 의해 다중 계통의 여러 트레인이 동시에 고장나는 사건을 말한다. 원전 신뢰성의 근간이 되고 있는 계통 및 기기의 다중성이 이 공통원인 고장에 의해 위협 받는 경우 전체 노심손상빈도를 크게 증가시킬 우려가 있으므로 이에 대한 철저한 분석이 요구되는 것이다.

공통원인 분석은 크게 네 단계로 나눌 수 있다.^[8]

- 계통 논리 모델 개발: 계통친숙화, 문제정의 및 논리 모델 개발
- 공통원인 기기군 파악: 정성적 분석 단계와 정량적 분석 단계로 나눌 수 있는데, 정성적 분석 단계에서는 과거 경험이나 공학적 지식을 이용하여 공통원인

고장을 유발할 수 있는 기기 및 메카니즘을 찾게 된다. 이 단계에서 다양한 공통원인이 고려된다. 한 기기의 고장이 다른 기기 고장을 유발시키는 경우, 설계 및 제작을 잘못된 경우, 기기의 보수 및 운전 절차가 잘못된 경우, 절차를 따르지 않고 잘못 조작한 경우, 환경의 이상 변화 및 기타 원인들이 분석되는 것이다. 정성적 분석 단계에서는 각 공통원인사건의 확률에 보수적인 값을 할당하여 계통 이용 불능도의 초기값을 계산하고 주요 사건을 선별한다.

- 공통원인 모델링과 데이터 분석: 첫단계로 공통원인 기본 사건을 정의하고, 분석에 사용할 확률론적 모형을 선택한다. 다음단계로 고장자료를 분류하고 선별하고 정해진 모형의 확률 모수를 추정한다. 정량적 분석을 위한 다양한 확률 모형이 개발되었으나, 그중 널리 쓰이는 방법으로는 β -factor 모델, M-GL(multiple greek letter) 모델 α -factor 모델 및 binomial failure rate(BFR) 모델등이 있다. β -factor 방법은 기기 고장율에서 차지하는 공통원인고장율의 비율을 β 라는 확률 모수로 정의하여 추정하는 방법으로서 공통원인 발생시 다중 트레인이 α -factor 방법은 이를 보완하여 트레인 수에 따라 공통원인에 의한 조건부 고장율을 추정하는 방법으로서 최근 널리 사용되고 있다. BFR 방법은 공통원인에 의한 shock 발생시 각 기기의 고장율을 binomial 분포를 이용하여 추정하는 방법으로서 또한 널리 사용되고 있다.

공통원인 고장자료는 그 수가 제한되어 있으므로 주어진 자료로부터 최대한의 정보를 얻어내야 한다. 반면 기기가 동시에 고장 나더라도 공통원인에 의한 것인지, 아니면 우연에 의한 것인지 철저한 분석이 필요하며, 분석대상계통에 적합한 자료만을 선별해서 이용하여야 한다. 공통원인고장은 다분히 발전소 고유의 특성이므로, 일반고장자료(generic data)의 이용은 부적절하며 초기 정량화시 참고자료 정도로 쓰고, 발전소 고유 자료 및 공학적 특성이 철저히 분석되어야 하므로 많은 시간과 노력이 요구된다.

- 계통정량화 및 결과 해석: 공통원인에 의한 다중기기 고장 사건의 하나의 기본 사상으로 취급되어 고장수목에 입력되며, 이에 따른 계통 정량화는 일반적인 고장수목 정량화 방법으로 수행될 수 있다. 정량화 이후 계통이용불능도에 큰 영향을 미치는 사건을 나열하고, 그 결과의 타당성을 검토해야 하며, 공통원인 확률 모수는 불확실성이 큰 만큼 그 변화에 따른 민감도 분석이 수행되어야 한다.

최종적으로 노심손상빈도에 큰 영향을 미치는 기본 사상이 선별되고 이에 대한 대응책을 마련하는 것이 공통원인고장 분석 나아가 확률론적 안전성 평가의 주요 목표가 되는 것이다.

최근 국내·외에서 수행된 PSA의 결과를 보면 공통원인에 의한 고장 사건이 노심손상빈도의 큰 비율을 차지하고 있다. 즉, 공통원인에 대한 다중기기의 고장은 안전성에 치명적인 것이다. 이를 방지하기 위한 대응책 마련 및 정확한 모델 개발 및 자료 처리방법의 개발이 동시에 요구되고 있으며, 이에 대한 노력이 세계 각 처에서 경주되고 있다.

2. Level-2 확률론적 안전성분석: 격납용기분석

격납용기 분석에서는 사고경위별로 노심손상으로부터 격납용기 파손전까지의 물리적 진전과정과 방사성핵종의 방출 및 이송현상을 분석하여 사고 경위별로 격납용기 파손정도 및 이에 따른 방사성핵종의 대기중으로의 방출량을 결정한다. 종래의 안전성분석에서는 노심손상후의 현상에 대해서는 거의 분석하지 않았으나 확률론적 안전성 분석에서는 이에 대한 노심, 압력용기, 원자로냉각재 계통 및 격납용기 사건수목을 구성·분석하여 격납용기의 파손모드를 사고경위별로 파악하고 격납용기 파손을 야기시키는 사고경위에 대해서는 언제, 얼마만큼의 격납용기 파손이 발생하는지도 아울러 평가한다.

격납용기 사건수목은 앞에서 언급한 원전계통 사건수목과 같은 방법으로 구성하며 노심손상후의 열수력학적 거동 및 방사성핵종의 재고량에 관한 분석방법은 종래의 안전성분석 방법과 유사하므로 별도의 상세 언급을 피하기로 한다.


3. Level-3 확률론적 안전성분석: 결말분석

결말분석은 사고로 인해 격납용기가 파손되어 방사성핵종이 대기중으로 누출될 경우의 피해를 즉각 치사율, 암사망률 및 재산피해로서 기술하는 데 이용한다. 결말분석을 수행하기 위해서는 격납용기로부터 대기중으로 방출되는 방사성핵종의 양결정, 이들의 대기중 이송현상분석, 방사능 피폭의 분석, 방사능 피폭에 따른 건강효과 분석 및 피해의 경제적 효과 분석 등을 수행한다. 이러한 업무수행에 있어 특정부지의 기상자료, 인구분포 자료 및 지질특성자료들을 통계처리하여 활용하며 종래의 피폭선량해석과 달리 평균적인 입장에서 피해만 평가하지 않고 각 사고로 인한 방사능 방출 카테고리별로 결말에 대한 결과를 분포 함수로 나타낸다.

Ⅲ. 결 론

확률론적 안전성분석방법은 사고의 발생요인을 철저히 파악하고 이들 사고요인 발생시의 사고피해를 가능성으로 예측할 뿐 아니라 중요 사고요인 파악, 중요 사고경위 파악, 중요 원전계통 및 취약점 파악에 매우 유용한 방법이다. 현재에는 모든 건설중이거나 운전중인 원전에 대한 확률론적 안전성분석을 수행함으로써 원전의 안전성을 입증하고, 파악된 설계 및 운전이 취약점을 수정하고 개선하여 궁극적으로 원전의 안전성을 보다 향상시킬 수 있도록 하고 있다. 또한 보수, 시험, 관리 등 운전효율에 영향을 미치는 부분을 원전의 안전성을 일정수준이상으로 유지하면서 최적화하는 방향으로 재조정 하는 등 원전 가동률 향상 방안 도출에도 널리 이용되고 있다.

參 考 文 獻

- [1] USNRC, "Reactor Safety Study: An Assessment of Accident Risks in the U.S. Commercial Nuclear Power Plants", WASH-1400, 1985.
- [2] 유건중, 채성기, "확률론적 안전성분석", 원자력학회지, 제19권 제2호, 1987.
- [3] USNRC, "PRA Procedures Guide, A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", NUREG/CR-2300, Vols. 1 and 2, Jan. 1983.
- [4] Ralph R. Fullwood, Robert E. Hall, "Probabilistic Risk Assessment in the Nuclear Power Industry", PERGAMON PRESS, 1988.
- [5] B. J. Bell, A. D. Swain, "A Procedure for Conducting A HRA for NPPS", NUREG/CR-2254, 1983.
- [6] G. W. Hannaman, J. R. Fragola, "Systematic Human Action Reliability Procedure", NP-3583, EPRI, 1984.
- [7] A. D. Swain, H. E. Guttmann, "Handbook of HRA with Emphasis on NPP Application", NUREG/CR-1278, 1983.
- [8] A. Mosleh et al., "Procedures for Treating Common Cause Failures in Safety and Reliability Studies", NUREG/CR-4780, 1988. 

筆者紹介



朴 昌 奎
 1951年 11月 28日生
 1974年 서울대 핵공학 전공(학사)
 1979年 서울대 핵공학 전공(석사)
 1982年 MIT 핵공학 전공(석사)
 1986年 Univ. of Michigan 핵공학
 전공(박사)

1974年~1976年 육군 중위
 1976年~1979年 한국원자력연구소 노심계통연구실
 연구원
 1984年~1989年 BNL 안전총괄실 연구원
 1989年 ~ 현재 한국원자력연구소 원자로안전평가실 실장

鄭 源 大 1959年 5月 15日生
 1983年 고려대학교 산업공학(학사)
 1987年 한국과학기술원 산업공학
 (석사)

1987年~1990年 8月 한국원자력연구소 원자로안전
 연구실 연구원
 1990年 9月~현재 한국원자력연구소 원자로안전평가실
 신입연구원