論 文 12-4-19

원자력발전소의 안전성 및 신뢰도 평가

Safety and Reliability Assessment for Nuclear Power Plants

정 원 대* · 황 미 정*
W.D. Jung · M.J. Hwang
(1997년 3월 14일 접수, 1997년 12월 12일 채택)

ABSTRACT

Probabilistic Safety Assessment(PSA) is an engineering analysis of the possible contributors to the risk from a nuclear power plant. It consist of three phases named as Level 1, 2 and 3. Level 1 PSA mainly focused in this paper is the phase of system analysis which includes the development of accident scenarios and the frequency estimation of each scenario. It covers also the system reliability analysis, component data analysis, and human reliability analysis. PSA have become a standard tool in safety evaluation of nuclear power plants. The main benefit of PSA is to provide insights into plant design, performance and environmental impacts, including the identification of dominant risk contributors and the comparison of options for reducing risk.

1. 서 론

오늘날 우리들이 살고있는 사회는 석유화학, 정유, 정밀화학 혹은 원자력발전소 등과 같은 고도의 기술집약적 대규모 장치 산업에 크게 의존하는 산업 사회로서 중대 산업사고의 잠재적 위험성을 내재하고 있다. 기술의 고도화 및 안전설비의 설치 등으로 사고의 빈도는 높지 않으나 일단 화재, 폭발, 독극물 혹은 방사능물질의 누출과 같은 사고가 발생하면 시설의 파괴 혹은 오염으로 인한 경제적 손실은 물론 대규모 인명피해를 초래할 수 있는 가능성이 있다. 또한 이런 중대 산업재해는 주변 환경에 치명적 영향을 미칠 수 있어 환경에 대한 인식이 급격히 고조되고 있는 현대 사회에 커다란 문제를 야기시킬 수 있다.

이러한 중대 산업재해에 대한 대비로써 주요 위험설비에 대한 안전성을 평가하고 확인된 위험 요소를 사전에 제거하거나 만약의 사고에 대한 비상대책수립 등 체계적인 안전대책을 수립

* 한국원자력연구소 종합안전평가팀

하여 시행할 필요성이 커지고 있다. 국내에서도 이와 관련하여 산업안전보건법을 개정하여 1996년부터 석유 화학공장 및 위험물질 취급 설비에 대하여 공정안전관리제도(Process Safety Management)를 전면적으로 시행하고 있다.

이와 같이 산업안전에 대한 관심이 고조되고 있는 상황에서 안전성 확보 및 증진에 일찍부터 많은 노력을 기울여온 원자력분야의 안전성평가 방법을 소개함으로써 산업체간의 안전평가 기술의 교류와 발전에 기여하고자 한다.

2. 원자력발전소 안전성 평가 개요

원자력산업에서의 안전성 및 신뢰성 분석을 이해하기 위해서는 우선 원자력산업이 타 산업과 어떤 점에서 유사하며, 어떤 점에서 차이가 나는지를 이해할 필요가 있다. 원자력산업, 특히 원자력 발전소(이하 원전)의 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. 원전은 발전 원리면에서 석탄이나 석유와 같은 화석연료를 연소시켜 발전하는 화력발전소와 큰 차이가 없다. 물을 끓여서 나오는 증기로 터어빈을 돌려서 발전하는 것은 같은 메카니즘이며, 단지 물을 끓이는 방법에서 우라늄을 사용하느냐 아니면 화석연료를 사용하느냐의 차이가 있을 뿐이다. 화력발전소는 공해문제가 큰 반면 원전에서는 핵연료에서 발생하는 방사능 물질의 외부 유출을 어떻게 막느냐 하는데 있다.

방사능의 외부 유출을 막기 위하여 원전은 크게 다섯 가지의 방호층을 갖도록 설계되었다. 즉 핵연료 펠릿이라고 부르는 새끼 손가락의 끝마디 정도 크기의 연쇄 핵반응이 직접 일어나는 핵연료 부분이 있다. 펠렛의 속에서 생성된 방사능은 그 속에 대부분 갖혀 있게 된다. 이것이 제1차 방호층이다. 이 핵연료 펠릿을 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 원자로 용기가 이 모두를 싸고 있어 제4의 방사능 방호층을 이루며, 마지막으로 약 1m 두께의 철근 콘크리트로 둘러싸인 격납건물이 있어 만약 제4의 방호층을 뚫고 나온 방사능이 있는 경우에라도 이를 외부 환경으로 유출되지 못하게 한다. 이러한 다섯가지의 방호층을 형성하는 개념이 바로 다중방호개념(Defense in Depth Concept)이다.

다중방호개념과 함께 원자력 안전을 확보하려는 신뢰도 관점에서의 노력이 중첩(Redundancy) 설계이다. 중첩설계는 위에서 설명한 각 방호층의 신뢰성을 높이기 위하여 도입된 설계 개념이다. 즉, 각 방호층의 보호를 위하여 2개에서 4개까지의 독립적(Independence)이고 다양화(Diversity)된 각종 공학적 안전장치들을 설치하는 개념이다. 뿐만 아니라 많은 안전관련 기기들이 고장이 발생해도 계통이 안전한 상태에 있게하는 Fail-Safe 개념하에서 설계되었다.

앞에서 언급한 바와 같이 원자력에서의 신뢰도분석은 이와 같은 원자력 고유의 특성이 유지된 상태에서 행해져 오고 있다. 따라서 신뢰도 분석은 독자적인 분야이기 보다는 원전의 종합 안전성 평가의 한 부분으로 수행되어 오고 있다. 원전의 안전성을 확보하고 확인하기 위한 방법으로는 전통적으로 결정론적인 안전성분석(Deterministic Safety Analysis) 방법이 사용되고 있는데, 이 방법은 발생가능한 중요 사고를 선정하고 이러한 사고가 발생하더라도 원전이 안전하다는 것을 확인하는 방법이다. 이때 설치된 안전계통의 정상적으로 기능을 발휘한다는 가정을 하게 되는데, 이러한 가정은 계통의 다중성 및 다양성 확보로 만족된다는 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 안전성평가(Probabilistic Safety Ass-

essment : PSA) 이다. PSA 기법은 1975년 완료된 WASH-1400[1]에서 처음 사용되었으며, 그 후 원자력산업의 안전성평가에 널리 이용되어 왔다. 확률론적 안전성평가 방법은 종래의 결정론적 분석에 의해서는 나타나지 않던 원전의 취약점을 파악, 개선할 수 있도록 함으로써 원전 안전성을 제고시키는데 큰 기여를 하였으며, 이제는 운전/보수 절차의 개선, 설계 개선, 운전원 교육, 부지 선정, 안전성 목표 설정 등 다양한 분야에 응용되고 있다.

3. 확률론적 안전성평가(PSA)

원전에는 앞에서 살펴본데로 많은 안전장치들을 중복 설치하여 사고의 발생을 최대한 방지하며, 사고가 발생하더라도 그 피해를 최소화하도록 설계되었다. 그러나, 안전계통을 다중 설치하고 계통의 신뢰도를 높여도 운전원의 실수나 부품의 작동 실패를 완전히 방지할 수는 없으며, 가능성은 매우 작지만 안전계통들의 작동불능으로 핵연료 손상(이하 노심손상)을 초래하는 사고가 발생할 수도 있다. 따라서 잠재적 원전사고를 사전에 예방하고 만일의 사고에 대한 대책 마련을 위해, 우선 원전에서 발생할 수 있는 가능한 사고는 어떤 것들이 있으며 그러한 사고의 발생 가능성 및 그로 인한 피해를 평가할 필요성 대두되었다.

PSA 업무란 원전에서 발생할 수 있는 모든 주요 노심손상 사고 시나리오들을 파악하고, 확률 이론에 근거하여 그 발생 빈도를 추정하며, 각 사고 시나리오에 대하여 예상되는 인적, 물적 피해를 정량적으로 평가하는 것이다[2,3]. PSA 수행 결과 어떤 사고 시나리오가 상대적으로 중요하며 어떤 계통이 발전소 안전성측면에서 중요한지를 파악할 수 있으며, 이러한 중요도에 의거하여 사고 대책은 물론 설계, 건설 및 운전 측면에서의 개선안을 도출할 수 있다[4,5].

PSA는 Fig. 1에서 보여 주는 바와 같이 크게 세가지 업무로 구분할 수 있다. 첫번째 업무는 계통신뢰성분석으로 사고 요인별로 노심손상에 이를 수 있는 사고 시나리오들을 파악하고 노심손상 발생빈도를 추정하는 단계이다. 이에는 일반적으로 사건수목(Event Tree)분석 및 고장수목(Fault Tree) 분석 기법이 이용되며, 이 단계가 완료되면 원전에서 발생할 수 있는 주요 사고 시나리오들과 그 발생빈도가 추정되어 대상 발전소의 안전성이 일차적으로 평가된다.

두번째 업무는 격납건물분석(Containment Analysis)으로 첫번째 업무에 파악된 각 사고 시나리오별로 노심손상 후 격납건물내의 압력과 온도, 방사능 물질 생성 양과 현상을 분석하는 단계이다. 여기에서는 사고 전개과정에서 격납건물의 파손 가능성을 분석하고 격납건물 파손시 주변 환경으로의 방사능 방출량을 계산한다.

세번째 업무는 결말분석(Consequence Analysis)으로서 노심손상 사고로 인하여 격납건물 파손시 대기중으로 방출되는 방사성 물질의 확산 범위 및 정도를 추정하고, 주변 오염으로 인한 사고 피해를 주민의 인체에 미치는 영향과 경제적 손실로 평가한다. 이 단계가 완료되면 대상 원자력발전소에 대한 위험성(Risk)이 정량적으로 평가된다.

앞에서 언급한 세가지 분석 단계를 거치면 원자력발전소에서 발생 가능한 사고의 발생 빈도 및 피해 정도를 사고 요인별, 사고 시나리오별로 파악할 수 있다. PSA라 하면 원칙적으로 이 세가지 업무를 통털어 일컫는 말이다. 그러나 PSA를 수행하는 목적에 따라 분석 업무를 제한적으로 수행할 수도 있다. 계통 신뢰도분석을 통한 노심손상빈도 계산까지를 Level-1 PSA, Level-1 PSA와 격납건물분석까지를 Level-2 PSA, 결말분석까지의 전 분석업무를 Level-3 PSA라고 구분하여 부르기도 한다. 본문에서는 원전 안전성평가에서 가장 중요하고 기본적인 업무인 Level-1 PSA의 분석 방법을 주로 정리하고, 격납건물분석, 결말분석은 간략히 소개하고자 한다.

3.1 Level-1 PSA(노심손상 사고 시나리오 분석)

Level-1 PSA 수행 목적은 원자력발전소에서 발생 가능한 모든 노심손상 사고 시나리오를 밝혀내고 그 발생빈도를 추정하는 것이다. 이를 위해 수행하는 주요 업무의 내용은 다음과 같다.

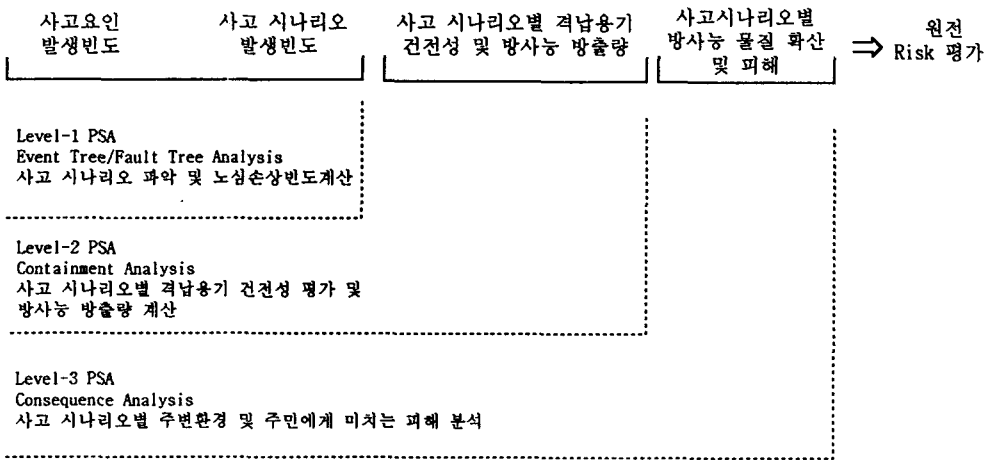


Fig. 1 Work scope of Probabilistic Safety Assessment (PSA)

발전소 친숙화: 대상 발전소의 설계, 운전 및 보수 등에 관련된 자료를 수집하고 친숙화하는 과정으로 계통의 특성, 구성 기기, 타 계통과의 연계성, 운전 및 보수 방식 등에 대한 모든 정보를 포함한다.

초기사건분석: 원자력발전소에서 발생할 수 있는 모든 종류의 사고 유발자를 파악하고 이에 대한 발전소 안전계통의 대응 방식을 평가하여 유사한 것끼리 그룹핑하여 사고 시나리오분석 대상이 되는 초기사건 목록을 확정한다.

사건수목분석: 선정된 초기사건들에 대하여 각 안전계통의 작동 성공 여부에 따른 사고 전개 시나리오를 개발한다. 이 과정을 통하여 노심손상을 초래하는 사고 시나리오가 결정된다.

고장수목분석: 개발된 각 사고 시나리오의 발생빈도를 평가하기 위해서는 각 관련 계통의 신뢰도 분석이 필요한데, 고장수목분석을 통하여 관련 계통들을 기기수준의 고장 논리로 표현하고 이를 근거로 계통의 이용불능도를 평가한다.

신뢰도 자료분석: 노심손상 발생빈도와 계통 신뢰도를 평가하기 위해서는 초기사건의 발생빈도 및 계통 고장수목에 모델링된 모든 사건에 대한 신뢰도 정보가 기본적으로 제공되어야 한다. 자료분석에는 다음과 같은 세부 신뢰도 정보가 포함된다.

- 초기사건 발생 빈도
- 기기의 기계적 고장율
- 기기의 보수/시험 빈도 및 시간
- 인간오류 확률
- 공통원인고장 확률

정량분석: 원자력발전소 PSA에는 방대한 양의 사고 시나리오 전개 논리와 계통 신뢰도 모형이 개발되는데, 정량분석에서는 이들 사고 시나리오와 계통 고장수목을 통합(Integration)하여 계통 신뢰도 및 최종 노심손상빈도를 추정한다. 정량분석에는 중요도분석, 불확실성분석, 민감도분석 등이 함께 수행된다.

PSA 업무에는 일반적으로 방대한 양의 계통 고장수목 및 신뢰도 자료가 관련되므로, 사고 시나리오 도출 및 고장수목분석, 정량분석 등 모든 과정에 걸쳐 전산 코드가 사용된다. 그림 2는 Level-1 PSA의 주요 업무 및 수행 절차를 간략히 보여주고 있다. 주요 분석 단계의 내용을 보다 상세히 살펴보면 다음과 같다.

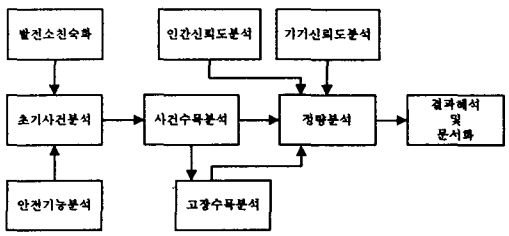


Fig. 2 Task flow of Level-1 PSA

1) 초기사건분석

사고 시나리오를 결정하기 위한 첫번째 단계는 원전의 노심손상을 초래할 수 있는 사고 시나리오들의 초기사건을 선정하는 것이다. 초기사건이란 정상 운전 중인 발전소의 불시적인 원자로 정지를 초래하는 기기 혹은 계통의 이상이나 인간오류를 의미한다. 원자로 정지란 운전변수들이 적정 운전 범위를 벗어나는 경우에 취해지는 보호조치이다. 따라서 초기사건이 발생하면 원자로의 보호 및 사고 방지를 위하여 안전계통들이 작동, 원자로를 정지시키고 노심 잔열을 제거하여 원자로를 안전하게 유지한다. 만일 초기사건 발생시 이들 안전계통들이 적절히 기능을 수행하지 못하면 사고로 이어질 수 있으므로 일단 이들 초기사건들이 향후 분석의 출발점이 된다.

초기사건에는 원전 내부적 요인에 의한 것과 지진, 홍수, 태풍 등과 같은 외부적 요인에 의한 것으로 구분되며, 다음과 같은 분석 절차에 의해 초기사건이 결정된다. 첫째 발전소의 안전기능(Safety Function) 을 저해할 수 있는 가능한 사고 유형들을 논리적으로 추적하기 위해 주 논리도(Master Logic Diagram) 를 개발하고, 둘째 단계에서는 앞에서 파악된 사고 유형에 대한 구체적 목록을 작성한다. 이 단계에서는 운전 및 사고 경험의 분석, 주요 기기에 대한 고장모드 분석(Failure Mode Effect Analysis), 타 PSA의 초기사건 목록 검토 등을 통하여 발생 가능한 모든 초기사건들의 목록을 작성한다. 마지막 단계에서는 사고 유형이나 진행 과정이 유사하며, 이들 사고로부터 원자로를 안전하게 정지시키기 위해 필요한 안전계통 및 그 성공기준이 동일한 초기사건들을 그룹화하여 최종 초기사건을 결정한다.

2) 사건수목분석(Event Tree Analysis)

사건수목분석이란 선정된 초기사건 각각에 대하여 사건수목을 구성하여 각 초기사건에 대하여 어떻게 사고가 전개되고 확산되어 노심손상이 발생할 수 있는지를 밝혀내는 작업으로, 노심손상을 초래하는 모든 중요 사고 시나리오들을 논리적으로 밝혀내는 과정이다. 이를 위해서 각 초기 사건별로 원전을 안전한 상태로 유지하기 위해 필요한 안전기능(Safety Function)을 파악하고 필요한 안전계통 및 운전원 조치를 정리하여 사건수목의 표제(Heading)로 정의한다. 초기사건 발생 후 각 표제의 성공 혹은 실패에 따라 이분수목(Binary Tree) 형태로 사고 시나리오를 전개하여 발생 가능한 노심손상 사고 시나리오를 논리적으로 구성한다.

사건수목 구성에서는 초기사건 발생 후 노심손상을 방지하기 위하여 필요한 안전계통들의 작동 성공, 실패에 따라 수 많은 사고 시나리오가 논리적으로 전개된다. 이들 사고 시나리오 중 어떤 사고조합들은 사고를 성공적으로 완화시키는 사고 시나리오가 될 것이며, 어떤 사고 시나리오들은 노심손상을 초래하는 사고조합들이 된다. 이를 판단하기 위하여 때로는 많은 열수력 사고해석을 수행하여야 하기도 한다. 또한 모든 가능한 사고 시나리오를 빠짐없이 밝히기 위하여는 초기사건 발생시 이에 관련되는 모든 계통들의 정확한 운전특성 및 운전원의 관련작업 파악은 물론 사고로 인해 초래되는 물리적 현상에 의해 생기는 계통들간의 상호 연관성 등에 대한 정확한 이해가 필요하다.

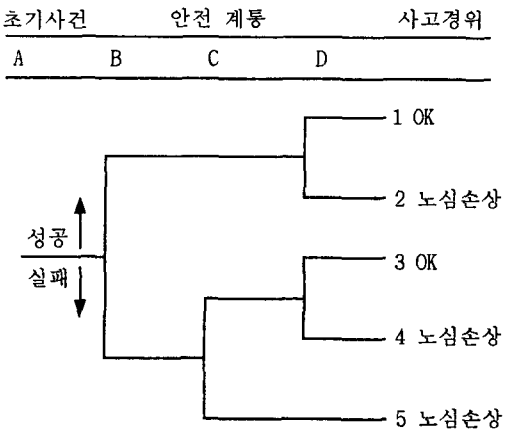


Fig. 3 An example of Event Tree

사건수목 구성 및 평가를 간단한 예를 통하여 살펴보면 다음과 같다. 초기사건 A가 발생하였을 때 사고의 방지 및 완화를 위하여 안전계통 B 및 D가 성공적으로 작동하든지, 만일 안전계통 B가 실패하는 경우 계통 C 및 D가 성공적으로 작동해야 한다면, 이런 상황에서 발생할 수 있는 관심있는 사고 시나리오는 Fig. 3에서

보는 바와 같이 5가지가 존재한다. 사고 시나리오 1은 초기사건 A 발생 후 계통 B, D가 모두 정상적으로 작동하여 성공적으로 사고를 종결시킨 경우이며, 사고 시나리오 3은 계통 B는 작동실패하였지만 다른 안전계통인 C가 성공적으로 작동하고 그 후 계통 D가 정상적으로 운전되어 노심손상을 방지한 사고 사나리오를 나타낸다. 그러나, 사고 시나리오 2, 4, 5는 계통 B, C, D 중 어느 하나 혹은 그 이상이 이용불능이어서 노심손상을 초래하는 사고 시나리오를 의미한다.

사고 시나리오 2, 4, 5로 인한 사고 발생 빈도를 계산하기 위해서는 우선 초기사건 A의 발생빈도(Frequency)와 계통 B, C, D의 작동실패 확률, 즉 이용불능도(Unavailability)를 알아야 한다. 초기사건 발생빈도는 과거 사고 자료를 조사하여 추정하며, 계통의 이용불능도는 다음에 언급할 고장수목분석을 통하여 산출한다. 만일 초기사건 A의 발생빈도가 Fr(A)=1.0E-3회/년이고 계통 D의 이용불능도가 Pr(D)=2.0E-3이라면, 사고 시나리오 2로 인한 노심손상 발생빈도는 Fr(A)*Pr(C)=2.0E-6회/년이 된다. 이와 같은 방식으로 사고 시나리오 4, 5에 대한 정량화를 수행하면, 초기사건 A로 인한 노심손상 발생 빈도를 추정할 수 있게 된다.

실제 원전 PSA의 사건수목 구성시에는 고려해야 할 안전계통 및 운전 조건들이 훨씬 많아 사건수목은 복잡하게 구성된다. 초기사건이나 사건수목 구성 방법에 따라서 다르나 하나의 초기사건에 대하여 대략 20~40여개의 사고 시나리오가 개발된다. 위의 예에서는 계통들간의 종속성이 없다고 가정하였으나, 많은 경우 초기사건과 계통간 혹은 계통들 사이의 종속성(Dependency)이 존재하므로 이를 모델링에 적절히 반영하고 평가하는 것이 매우 중요하다.

3) 계통 고장수목분석(Fault Tree Analysis)

앞에서 언급한 것처럼 원자력발전소의 노심손상빈도를 산출하기 위하여는 관련된 모든 계통들의 신뢰도를 분석하여야 한다. 원전에는 여러 종류의 안전계통들이 중복적으로 다중 설계되어 있으며, 계통의 규모가 크고 운전 조건 및 방식이 복잡하게 상호 연관되어 있으므로 계통 신뢰도분석은 쉬운 작업이 아니다. 또한 동일 계통일지라도 사고 시나리오에 따라 계통 성공기준이 달라지기 때문에 모든 사고 시나리오의 발생 빈도를 추정하기 위하여는 방대한 양의 계통 신뢰도분석이 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, 초기작동에는 성공하더라도 주어진 임무시간(Mission Time) 동안 연속작동에 실패하는 것을 의미한다. 계통의 작동불가능 요인으로는 여러가지가 있을 수 있다. 관련 계통내의 각종 부품의 고장, 계통내 여러 기기의 작동 불능을 초래하는 전기, 기기냉각수, 공기냉각, 계기/제어 등과 같은 보조계통(Support System)들의 고장은 물론 시험 및 보수작업과 관련된 인간오류(Human Error) 등이 계통의 이용불능을 초래한다.

계통신뢰도분석을 위하여 여러가지 방법이 개발되어 있으나, 원전의 계통신뢰도는 일반적으로 방대하고 복잡한 시스템의 정량적 분석에 적합한 고장수목분석 기법을 통하여 평가하고 있다. 고장수목분석은 계통이 작동불능하게 되는 직접적인 요인들을 연역적이고 도식적인 방법으로 분석하고 이를 Boolean 방정식으로 표현한 후, 각 요인들의 발생 확률값을 대입하여 계통의 이용불능도를 계산하는 방법이다. 고장수목 구성시에는 관련 계통의 부품의 고장은 물론 시험, 보수 및 계통의 운전과 관련된 운전원 오류도 고려하게 되므로 기기고장률이나 인간오류 확률값과 같은 신뢰도 자료의 확보가 중요하게 된다. 또한 고장수목분석시에는 공통원인고장이나 타계통과의 연관성 등을 적절히 모델링하는 데 주의를 기울여야 한다

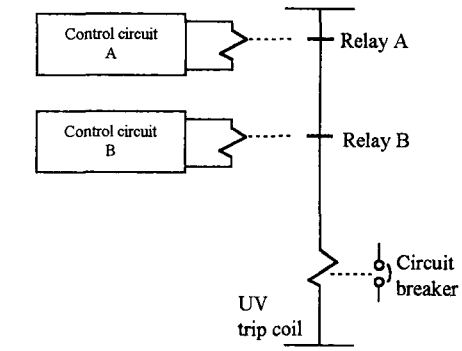
고장수목의 구성 및 분석을 간단한 예를 통해 설명하면 다음과 같다. 보다 상세한 내용은 관련 참고문헌[2,6]에 상세히 기술되어 있다. 먼저 분석 절차는 다음과 같다.

- ▶ 분석대상계통의 성공기준을 근거로 계통의 기능 실패 조건을 결정하고 이를 고장수목의 정점사건(Top Event)으로 정한다.
- ▶ 정점사건이 주어지면 이러한 정점사건이 일어날 수 있는 직접적인 요인들을 연역적방법에 의하여 파악하고 이들 요인들을 AND 또는 OR 게이트(Gate) 등의 논리자로 표시한다.
- ▶ 정점사건이 일어날 요인 파악은 모든 요인들이 부품의 기계적 고장이나 인간오류 등과 같이 신뢰도 자료가 제공되는 기본사건(Basic Event)으로 표현될 때까지 계속한다.
- ▶ 고장수목이 구성된 후에는 이를 Boolean 방정식으로 표시한다.
- ▶ Boolean 방정식을 풀어서 정점사건을 유발하는 기본사건들의 조합인 최소단절집합(Minimal Cut Set)을 결정한다.
- ▶ 기본사건들의 신뢰도 자료를 대입하여 최소단절집합들의 이용불능도를 계산하고, 정점사건에 대한 모든 최소단절집합들의 이용불능도를 더하여 계통 이용불능도를 구한다.

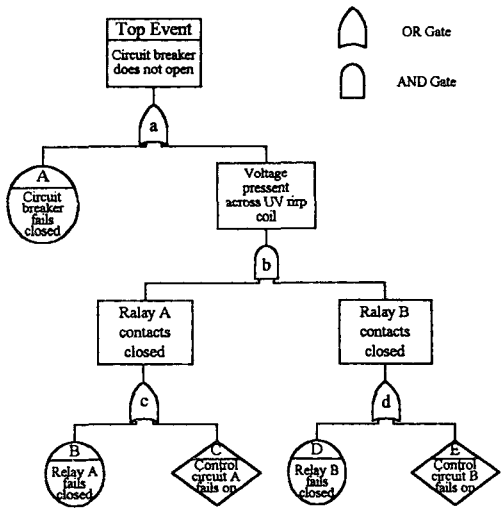
고장수목분석을 이해하기 쉽게 하기 위하여 Fig. 4(a)와 같은 구조를 갖는 circuit breaker 의 trip 고장을 살펴보기로 한다. Circuit breaker trip 실패는 "circuit breaker does not open"으로 표시할 수 있으며 이를 고장수목의 정점사건으로 잡는다. 이 정점사건을 유발시킬 요인들을 연역적으로 파악해 보면, circuit breaker가 열리지 않는 경우는 circuit breaker 자체가 닫혀 있는 상태로 고장이 났거나 UV trip coil에 전류가 흐르는 경우로 표시할 수 있다. 다음에 UV trip coil에 전류가 흐르는 경우는 다시 relay A와 B가 동시에 닫혀 있는 것으로 볼 수 있다. 다시 relay A와 B가 닫혀있는 경우는 relay 자체 고장으로 인한 고장과 control circuit의 고장에 따른 작동으로 인한 경우로 파악할 수 있다.

이런 논리전개를 고장수목으로 표현하면 Fig. 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 게이트를, 하부사건들중 어느 하나만 발생하여도 상부사건이 일어나는 경우에는 OR 게이트를 사용하여 정점사건에 대한 고장수목을 구성한다.

Fig. 4(b)에서 보는데로 게이트는 영문 소문자로 기본사건은 영문 대문자로 표시하였을 때, 이를 이용하여 정점사건 a를 Boolean 수식으로 표현하면, $a=A+b=A+cd=A+(B+C)(D+E)$ 이 된다. 이를 Boolean 대수를 이용하여 정리하면, $a=A+BD+BE+CD+CE$가 되며, 이로부터 정점사건 a를 유발하는 기본사건의 조합으로 A, BD, BE, CD, CE가 얻어지며 이들 모두가 정점사건 a의 최소단절집합이 된다.



(a) Circuit breaker trip 계통



(b) Circuit breaker trip 고장수목

Fig. 4 An example of Fault Tree for Circuit Breaker Trip System

만일 각 기본사건들의 발생확률값이 Pr(A)= 0.001, Pr(B) = Pr(C) = Pr(D) = P(E)=0.02라면, Pr(a)=0.001+0.02×0.02+0.02×0.02+0.02×0.02 +0.02×0.02=0.0026로 되어 정점사건 a의 발생 확률, 즉 circuit breaker trip 실패 확률은 0.0026이 된다. 정점사건 a의 이용불능도 계산시에 희귀사건근사(Rare Event Approximation), 즉 P(AUB) P(A)+P(B), 가정이 사용되었다.

4) 신뢰도 자료분석

신뢰도 자료분석은 사건수목과 고장수목에 모델링된 모든 기본사건에 대한 신뢰도 자료, 즉 빈도 및 확률값을 분석하는 과정이다. PSA 결과의 신뢰성은 사용된 데이타의 정확도에 의해 좌우되므로 신뢰도 자료분석 및 데이타베이스 개발은 PSA의 핵심 업무 중 하나이다. PSA 수행에 필요한 신뢰도 자료는 다음과 같은 것들이 있다.

▶ 초기사건 빈도
▶ 기기고장률
▶ 공통원인고장확률
▶ 인간오류확률
▶ 보수/시험 빈도 및 기간

신뢰도 자료분석은 PSA과제의 특성에 따라 업무 범위가 상당히 달라질 수 있다. 운전 중인 발전소에 대한 PSA인 경우에는 발전소 고유 운전 이력을 조사하여 분석에 반영해야 하기에 많은 시간을 투입하여 운전 데이타 및 고장 데이타를 수집, 분석하여야 한다. 그러나 대부분의 경우 충분한 양의 고장 데이타를 찾을 수 없기에 전세계적으로 원자력분야에서 사용되는 신뢰도 자료를 근거로한 일반데이타(Generic Data)와 발전소 고유데이타(Plant Specific Data)를 통계적으로 처리하여 사용하고 있다[7]. 설계 중인 원전의 경우에는 운전 경험이 없으므로 일반 데이타원을 근거로한 신뢰도 데이타 베이스를 사용한다.

신뢰도 자료 중에서도 특히 인간오류 확률을 평가하는 인간신뢰도분석(Human Reliability Analysis)[8]과 동일한 여러 기기를 동시에 이용 불가능하게 하는 공통원인고장(Common Cause Failure)[9]에 대한 분석이 상대적으로 매우 중요한 것으로 알려졌다. 이 두 분야는 신뢰도 자료분석에서도 각각 별도의 독립적인 업부 분야로써 여러 분석 기법들이 사용되고 있으나 아직 분석 결과에 대한 불확실성이 높아 분석 방법론에 대한 연구가 계속 진행 중에 있다.

5) 정량분석

정량화 단계에서는 이전 단계에서 수행된 모든 결과물을 조직적으로 통합하여, 노심손상을 초래하는 기본사건 조합들을 파악하고 그로 인한 노심손상빈도를 정량적으로 평가한다. 사건수목분석 단계에서 간략히 설명하였듯이 정량화에 주된 작업은 각 사고 시나리오들에 대한 Boolean 수식을 구하고, 이를 통하여 해당 사고 시나리오를 일으키는 최소단절집합(초기사건과 기본사건들의 조합)들을 파악한 후, 초기사건 발생빈도와 각 기본사건들의 발생 확률값을 대입하여 사고 시나리오 발생빈도를 구하는 것이다. 모든 사고 시나리오에 대한 정량화 결과를 합하면 총 노심손상빈도가 계산된다. 또한 각 사고 시나리오들에 대한 최소단절집합들을 검토하여 사건수목 및 고장수목 전개논리가 적절히 모델링 되었는지를 확인하는 정성분석도 이 단계에서 함께 수행한다.

PSA 정량화는 일반적으로 예비정량화와 최종정량화 두 단계에 거쳐 수행한다. 설계에 대한 개념적 평가나 주요 영향인자를 파악하기 위하여 간략한 모델과 보수적 데이타를 사용하여 예비분석을 수행하며, 상세 설계 자료와 예비정량화를 통해 밝혀진 논리적 혹은 신뢰도 데이타 사용의 문제점을 수정하여 최종정량화를 수행한다. 사용 데이타의 불확실성을 고려한 불확실성 분석, 주요 영향인자 및 설계 개선 항목에 대한 민감도분석과 중요도분석도 정량분석의 일부로 수행된다. 정량화 단계에는 일반적으로 방대한 양의 사건수목 및 고장수목 논리와 신뢰도 자료가 사용되기 때문에 전산 코드를 사용하여 정량분석을 수행한다.

3.2 Level-2 PSA : 격납건물분석

격납건물분석에서는 사고 시나리오별로 노심손상으로부터 격납건물 파손전까지의 물리적 진전과정과 방사성핵종의 방출 및 이송현상을 분석하여 사고 시나리오별로 격납 용기 파손정도

및 이에 따른 방사성핵종의 대기중으로의 방출량을 결정한다. 종래의 안전성분석에서는 노심손상 후의 현상에 대해서는 거의 분석하지 않았으나 확률론적 안전성평가에서는 이에 대한 노심, 압력용기, 원자로냉각재 계통 및 격납건물에 대한 분석을 수행하여 격납건물의 파손 모드를 사고 시나리오별로 파악하고 격납건물파손을 야기시키는 사고 시나리오에 대해서는 언제, 얼마만큼의 격납건물 파손이 발생하는지도 아울러 평가한다. Level-2 PSA는 원자력 고유의 안전성분석 영역이므로 별도의 상세한 언급은 생략한다.

3.3 Level-3 PSA : 결말분석

결말분석은 사고로 인해 격납건물이 파손되어 방사성핵종이 대기중으로 누출될 경우의 피해를 즉각 치사율, 암사망률 및 재산피해 등으로 평가하는 단계이다. 결말분석을 수행하기 위해서는 격납건물로부터 대기중으로 방출되는 방사성핵종의 양과 이들의 대기 중 이송현상분석, 방사능 피폭 분석, 방사능피폭에 따른 건강효과 분석 및 피해의 경제적 효과 분석 등을 수행한다. 이러한 업무 수행에 있어 특정부지의 지리적 정보, 기상자료, 인구분포 및 지질특성 자료들을 통계 처리하여 활용하며 종래의 피폭선량 해석과 달리 평균적인 입장에서의 피해만 평가하지 않고 각 사고로 인한 방사능 방출 카테고리별로 분석 결과를 분포 함수로 나타낸다.

4. 결 론

PSA는 중대 산업재해를 초래할 수 있는 산업설비에 대하여 발생 가능한 모든 사고 시나리오들을 파악하고, 이들 사고 시나리오의 발생빈도 및 사고로 인한 피해 정도를 정량적으로 평가하는데 매우 유용한 기법이다. 또한 시스템 전체 측면에서 중요 사고요인 및 사고 시나리오를 파악하거나, 안전성 측면에서 계통 및 기기의 상대적 중요성을 평가하고 설계 및 운전상의 취약점을 파악하는데 PSA는 널리 사용되고 있다. 현재 국내에서 건설중이거나 운전중인 모든 원전에 대하여 PSA를 수행하므로써 원전의 안전성을 입증하고, 평가 결과로 도출된 설계 및 운전 취약점을 개선하여 궁극적으로 원전의 안전성을 제고시키고 있다. 또한 원전의 안전성을 일정 수준이상으로 유지하면서 보수 및 시험 일정을 최적화하는 등 원전의 관리 효율 및 운전 가동률 향상을 위해서도 활용되고 있다.

한국원자력연구소에서는 안전성평가 및 신뢰도분석에 사용되는 전산코드 KIRAP (KAERI Integrated Reliabililty Assessment code Package)[10]을 개발하여 PSA 수행에 사용하고 있으며, 그 우수성이 국제적으로도 인정되어 1994년 미국 전력연구원인 EPRI에 수출하기도 하였다. 현재 신뢰도분석 기술의 고도화, 인간신뢰도분석 기술 개발, 국내 신뢰도 자료 처리 및 데이타베이스 구축을 위한 연구와 PSA 응용을 위한 Risk Monitor 개발이 진행 중에 있다.

신뢰도 분석 및 산업체 안전성에 대한 관심이 고조되고 있는 상황에서 원전의 안전성평가 및 제고를 위해 많은 노력을 기울여온 원자력분야의 안전성평가 업무를 소개함으로써 국내 산업체간의 안전평가 기술의 교류와 확산 및 정보교환의 활성화에 도움이 되었으면 하는 바램이다. 원전에 적용되는 안전평가 기술의 산업체 적용은 복잡한 위험 설비에 대한 보다 객관적이고 종합적인 안전성평가를 가능하게 하며, 이에 근거한 설비개선 및 운전관리의 최적화를 통하여 산업재해를 예방하고 궁극적으로 위험 설비의 안전성을 제고할 수 있을 것으로 기대된다.

참 고 문 헌

1) USNRC, "Reactor Safety Study : An Assessment of Accident Risks in the U.S. Commercial Nuclear Power Plants", WASH-1400, 1975.
2) 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.
3) IAEA, "Procedure for Conducting PSA of Nuclear Power Plants", Safety Series No. 50-P-4. 1992.

4) Ralph R. Fullwood, Robert E. Hall, "Probabilistic Risk Assessment in the Nuclear Power Industry", PERGAMON PRESS, 1988.
5) EPRI, "PSA Application Guide", EPRI TR-105396, 1995.
6) USNRC, "Fault Tree Handbook", NUREG-0492, 1981.
7) 한국원자력연구소, "일반 기기신뢰도 자료 조사/비교 및 PSA 수행용 일반 데이타베이스 구축", KAERI/TR-364/93. 1993.
8) USNRC, "Handbook for Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", NUREG/CR-1278, 1983.
9) USNRC, "Procedures for Treating Common Cause Failures in Safety and Reliability Studies", NUREG/CR-4780, Vol. 1, 1988.
10) 한국원자력연구소, "KIRAP(KAERI Integrated Reliability Assessment code Package) Ver2.0 사용자 설명서", KAERI/TR-361/93. 1993.