확률론적 안전성 평가 개요

양 준 언 | 한국원자력연구소 종합안전평가부

1. 확률론적 안전성 평가의 역사

사람들의 안전을 위협하는 위험 요소는 인류 사회가 시작된 이후 항상 존재하여 왔다. 과거의 시절에는 질병, 맹수, 지진 등 자연적인 위험 요소가 많았던 반면에 현대의 산업 사회에서는 자동차, 화학공장, 원자력발전소 등 인간이 만든 산업 설비에 의한 인위적 위험 요소가 많이 증가하였다.

이와 같이 인간이 만든 산업 설비에서 발생하는 인위적 위험은 산업 사회가 발전함에 따라 증가되는 편리성에 부수되는 필요악이라고도 할 수 있다. 따라서, 인공 설비로 인해 초래되는 위험은 그 설비가 사회에 제공하는 편리성의 정도에 따라 사회에 수용될 수도 있고 거부될 수도 있다. 즉, 산업 설비가 사회에 제공하는 편리성이 그 산업 설비에 의한 위험도(Risk)보다 클 때만이 사회가 그 산업 설비를 수용하게 된다.

이와 같은 측면에서 산업 설비의 위험도를 평가할 필요성이 제기되었으며, 이를 위하여 본 논문에서 소개할 확률론적안전성평가(Probabilistic Safety Assessment: PSA) 등 다양한 방법이 개발되었다 [1].

산업 설비의 위험도 평가를 위하여서는 먼저 "위험도"이라는 개념을 정량적으로 정의할 필요가 있다. 이와 같은 관점에서 위험도 평가에서는 일반적으로 위험도를 다음 식과 같이 발생가능성(Likelihood 혹은 Frequency)과 결과(Outcome 혹은 Consequence)의 곱으로 정의된다.

위험도 = 사고 발생 가능성 x 사고 영향

PSA는 1960년대 영국에서 화학 공장의 안전성 평가를 위하여 시작된 이후 미국의 항공우주국에서 우주선의 안전성을 평가하기 위하여 사용되었다. 현재 PSA 방법은 여객/화물 철도, 암모니아 저장 설비, 유조선 및 원자력발전소 등 매우 다양한 분야에서 광범위하게 사용되고 있다. 비록 동일한 평가 방법이기는 하지만 화공 산업계에서는 PSA를 QRA(Quantitative Risk Assessment)라고 부르며, 해운, 선박 산업계의 경우 이를 FRA(Formal Risk Assessment)라고 부르기도 한다. 즉, PSA 방법은 위험도 평가가 필요한 어떤 설비, 계통에서도 사용이 가능한 방법이다.

비록 PSA가 많은 장점을 갖고 있는 위험도 평가 방법이기는 하나, 또한, 몇 가지 제약점도 갖고 있다. 즉, 일반적인 PSA 방법은 평균적인 위험도만을 평가할 수 있다. 달리 이야기하면, PSA 방법은 주로 년간 평균 위험도와 같이 특정 기간 동안의 평균 위험도만을 평가하며, 어떤 특정 순간의 위험도를 평가하기 위하여서는 그 순간의 설비 특성을 반영한 PSA 분석이 다시 수행 되어야 한다.

또한, PSA 평가 결과의 정확성은 PSA에 사용되는 고장 자료 등 자료의 신뢰성에 의하여 많은 영향을 받는다. 따라서, PSA에서 나온 위험도 평가 결과를 사용할 때는 이와 같은 PSA의 한계점을 명확히 인식하고 있어야 한다.

다음 장에서는 원자력 발전소에의 적용예를 기준으로 PSA의 전반적인 개념에 대하여 간략히 기술하였다.

2. 확률론적 안전성 평가의 개요 : 원전 적용예를 중심으로

PSA는 앞에서 기술한 바와 같이 표시되는 원전의 위험도를 평가하기 위하여 사용되는 방법이다. 현재 PSA 방법은 원전의 설계, 운전 및 정비 등을 종합적으로 고려하여 원전의 안전성 평가 및 가장 효과적인 안전성 향상 방안을 도출하는 방법으로 인식되어 세계적으로 광범위하게 활용되고 있다. 이는 1979년도에 발생한 미국의 TMI-2 사고가 원전에 대한 최초의 종합적인 PSA인 WASH-1400에서 이미 예견 되었음이 밝혀지면서 PSA의 중요성 및 활용성이 밝혀졌기 때문이라고 할 수 있다.

원자력발전소에 대해 수행되는 PSA의 종류에는 내부사건 PSA와 외부사건 PSA가 있다. 외부사건 PSA는 지진, 홍수, 화재 등 자연 재해에 의해 발생하는 원전의 위험도를 평가하는 작업이다. 반면에 내부사건 PSA는 기기, 계통의 무작위 고장(Random Failure)에 의해 발생하는 원전의 위험을 평가하는 작업이다.

내부사건 PSA는 다시 전출력 운전시의 PSA, 저출력/정지시 PSA 등으로 구분할 수 있다. 전출력 PSA는 원전이 100%의 출력으로 운전하고 있을 때의 위험을 평가하며, 저출력/정지시 PSA는 원전의 출력이 100% 미만이거나 정비 등을 위하여 정지한 기간 중의 위험을 평가한다.

일반적으로 PSA는 다음과 같은 5가지 절차를 통하여 수행된다.

- 사고 빈도 평가(Accident Frequency Analysis)
- 사고 발전 경위 분석(Accident Progression Analysis)
- 위험도원 평가(Source-Term Analysis)
- 소외 영향 분석(Off-site Analysis)
- 위험도 평가(Risk Calculation)

원자력발전소에 대한 PSA는 흔히 세 단계(Level 1~3)로 구분된다. 즉, 위의 5가지 절차 중 "사고 빈도 평가"까지를 1단계(Level 1) PSA라고 칭하며, "사고 발전 경위 분석" 및 "위험도원 평가"를 2단계(Level 2) PSA라고 칭한다. 마지막으로 "소외 영향 분석"을 3단계(Level 3) PSA라고 칭한다. 세 단계 PSA의 각 단계별로 도출되는 주요 평가 결과는 다음과 같다.

- **1단계 PSA(Level 1 PSA)**: 발전소 내의 사고로 인한 노심 손상빈도를 결정한다.
- **2단계 PSA(Level 2 PSA)**: 1단계 PSA결과를 이용하여 격납용기의 반응을 평가하고, 궁극적으로는 격납용기 밖으로의 방사능 유출빈도를 결정한다.
- **3단계 PSA(Level 3 PSA)**: 2단계 PSA결과를 이용하여 발전소 외부에서의 사고 결과를 평가하고, 최종적으로 위험도를 추정한다.

위의 세 단계 PSA 중 가장 기본이 되는 1단계 PSA의 수행 과정이 그림 1에 나와 있다. 그림 1에 나와 있는 각 요소에 대한 설명은 다음에 기술되어 있다.

(1) **초기 사건**(Initiating Event)

: 원전의 중대 사고로 발전될 수 있는 원전의 과도상태를 유발하는 사건으로서 사건 수목(Event Tree) 분석의 시작점이 된다. 초기 사건의 도출은 기존 사고 이력 및 기존 분석에서 고려된 초기 사건을 조사하거나 FMEA(Failure Mode & Effect Analysis)나 Master Logic Diagram 분석 등 논리적 분석을 통하여 도출된다. PSA에서 고려하는 초기사건의 예로는 원자로의 불시 정지, 지진, 폭풍 등이 있다.

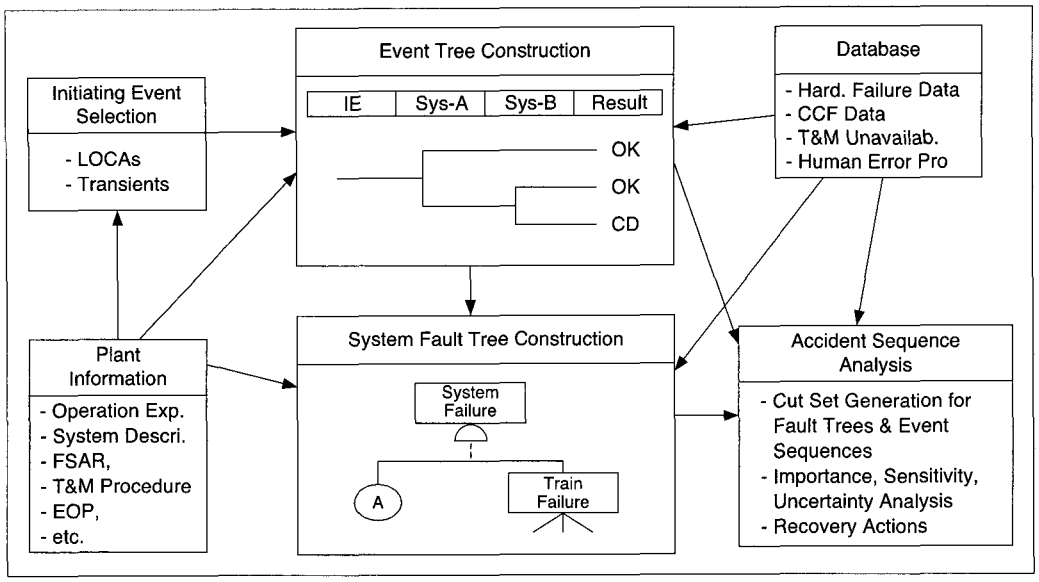

그림 1. 1단계 PSA 수행 절차

(2) 사건 수목(Event Tree: ET)

: 하나의 사건 또는 사고가 발생시 이를 완화시킬 수 있는 계통, 기기, 인적행위 등 각 요소가 요구되는 시간적 순서대로 각 요소를 모델하여 각 사고 경위의 빈도를 정량화하는 분석 방법으로 다양한 사고결과가 나타나는 사건의 전개과정 추적에 적절한 방법이다. 일반적으로 각 초기 사건에 대하여 한 개의 사건 수목이 개발된다. 예를 들어 그림 1의 ET에서 보듯이 어떤 초기 사건 IE가 발생하면 이의 영향을 완화할 수 있는 Sys-A, Sys-B의 성공/실패 여부에 따라 사고의 전개 과정이 달라지게 된다. 즉, 그림 1의 ET는 IE 발생 후 Sys-A나 Sys-B 중 하나만 성공적으로 가동되면 사고가 안전하게 종결되고, Sys-A와 Sys-B 둘다 고장이 나면 원전에 중대 사고가 발생한다는 것을 나타낸다.

(3) 고장 수목(Fault Tree)

: 특정 계통의 이용불능과 같이 사전에 정의된 정점 사건(Top Event)이 발생하는 원인을 추적하여 모델 및 정량화를 하는 연역적(Deductive) 분석 방법으로 정해진 사고 결과의 원인 추적에 적절한 방법이다. PSA에서는 주로 사건 수목에 나타나는 특정 계통(그림 1의 ET의 Sys-A, Sys-B 등)이 이용 불가능해지는 원인을 규명하는 데 사용된다.

일반적으로 고장 수목은 기본 사건(Basic Event)과 논리 게이트(Gate)로 구성이 된다. 기본 사건은 더 이상 하부의 원인이 없는 최종 고장 원인으로 펌프, 밸브 등 기기 고장, 인간 실수 등이 이에 해당된다. 논리 게이트는 이들 기본 사건의 결합 조건을 나타내는 것으로 예를 들어 어떤 두 기본 사건이 동시에 발생하여야 상위의 사건이 유발되는 경우는 이들 두 기본 사건을 AND Gate로 결합함으로써 표시한다.

고장 수목의 구성 예가 그림 2에 나와 있다. 그림 2에 나와 있는 예제 계통은 두 계열로 이루어진 계통으로, 펌프 P-1A와 밸브 V-1A가

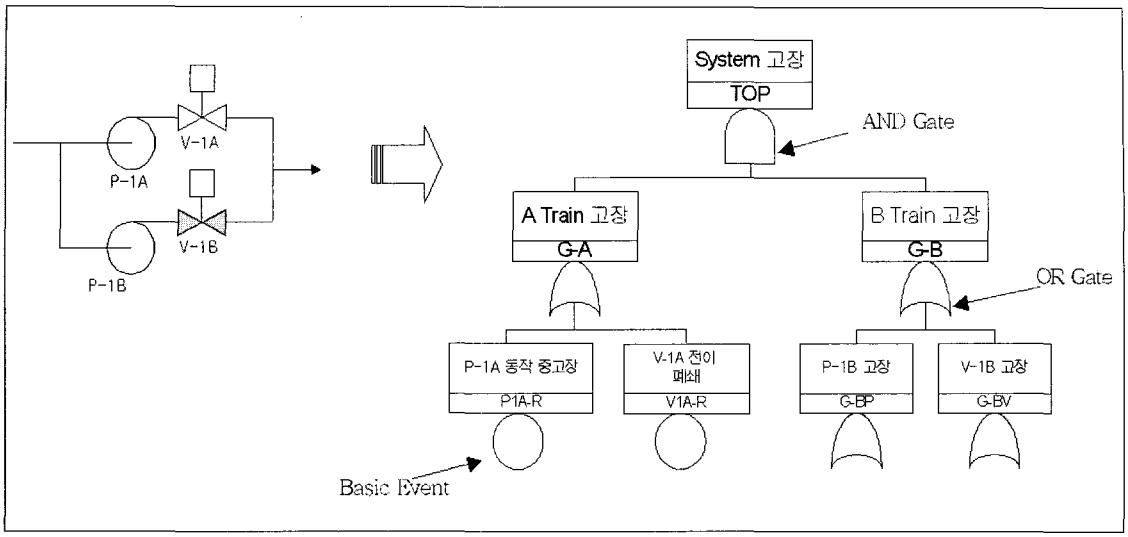

그림 2. 고장 수목 작성 예

있는 계열은 가동 중인 계열이며, P-1B와 V-1B로 이루어진 계열은 대기 중인 계열이다. 이 예제 계통이 기능 수행을 실패하는 경우는 A 계열과 B 계열이 동시에(AND)에 실패하는 경우이다. 따라서, 고장 수목의 정점 사건(예제 계통의 기능 상실) 바로 밑에는 A 계열과 B 계열이 동시에 실패하여야 한다는 것을 나타내는 AND Gate로 A 계열과 B 계열의 실패를 결합하고 있다. A 계열의 기능 상실은 펌프 P-1A와 밸브 V-1A 두 기기 중 하나만 실패하여도 발생된다. 따라서, 이 경우에는 펌프 P-1A와 밸브 V-1A가 OR Gate로 연결되어 표시된다. 고장 수목은 기본 사건들의 개별적인 고장 확률 값과 결합되어 계통의 기능 상실 확률을 계산하는 데 사용된다.

(4) 사고 경위 정량화

(Accident Sequence Quantification)

: 사고 경위 정량화는 초기 사건의 발생 빈도, 사건 수목의 노심 손상 유발 사고 경위 및 각 고장 수목의 기본 사건을 연계하여 노심 손상을 유발시킬수 있는 기본 사건의 집합(Minimal Cut Set: MCS)과 그 발생 빈도를 계산하는 과정이다. 이 과정에는 Boolean 논리 연산이 사용된다.

예를 들어 앞에서 기술된 고장 수목 예의 MCS는 펌프 P-1A와 P-1B의 동시 고장 등이 된다.

PSA의 결과로 나오는 이와 같은 MCS를 검토함으로써 어떤 기기, 인간 행위의 조합이 원전의 안전성에 가장 큰 영향을 미치며 그와 같은 조합 중 어떤 것을 개선하는 것이 가장 비용-효과적으로 원전의 안전성을 개선할 수 있는가 등을 분석할 수 있다.

3. 결론

본 논문에서는 원전에의 적용예를 통하여 PSA에 대한 개괄적인 소개를 하였다. PSA 방법은 위에서 설명하였듯이 원자력 발전소에서 발생 가능한 초기 사건, 사고 발전 경위, 계통의 고장 확률 등을 논리적

으로 결합하여 원전의 중대사고를 유발할 수 있는 가능한 모든 경우의 수를 찾아내는 방법이라고 할 수 있다.

원자력 산업에 있어 PSA는 원래는 원전의 안전성 평가를 위하여 도입이 되었으나 근래에 들어서는 "위험도 정보 활용(Risk-informed Application)"을 통하여 원전의 검사, 운영 지침, 품질 관리 등에 더욱 광범위하게 사용되고 있다.

서론에서 기술하였듯이 PSA 방법은 모든 산업 설비에 적용가능하나, 각 산업의 특성에 따라 방법론을 조절하여 쓸 필요가 있다. 또한 PSA 결과를 활용함에 있어서는 분석에 사용된 방법론 및 자료의 한계 등을 명확히 인식하고 이에 따른 북확실성을 고려하여 사용하여야 한다.

참고문헌

1. 박창규, 하재주, "확률론적 안전성 평가," 2003, 브레인코리아