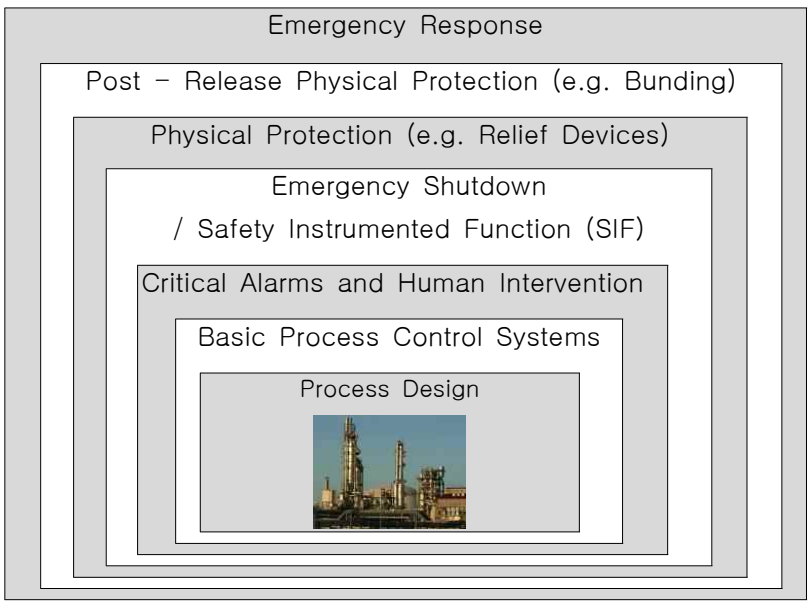
방어선(LOD)/방호계층(LOP)을 사용하는 위험성평가기법

1. 머리말

국내에 PSM(공정안전보고서) 제도가 도입된 후 대상사업장에서는 주기적으로 위험성평가를 수행하여 위험을 관리하고 있다. 많은 사업장에서는 HAZOP과 같은 정성적 위험성평가기법을 이용하며, 특별히 추가적인 분석이 필요하다고 판단되는 일부 시나리오에 대해서는 결함수 분석(Fault Tree Aanalysis), 사건수 분석(Event Tree Analysis), 사고결과 영향분석(Consequence Analysis)과 같은 정량적 위험성평가를 통해 위험을 분석하여 관리하고 있다. 그러나 대다수 사고시나리오에는 위험의 크기 및 기존에 설치된 안전장치에 대한 평가가 미흡하고 각 시나리오가 충분히 분석되었는지 판단하기 어렵다. 따라서 방호계층(Layers of Protection, 이하 LOP) 또는 방어선(Lines of Defence, 이하 LOD)과 같은 방호층 개념을 사용하게 되었다. 본 고에서는 LOD 또는 LOP의 개념, 그리고 이런 개념을 이용한 위험성평가기법의 소개 및 유용성에 대해 살펴보고자 한다.

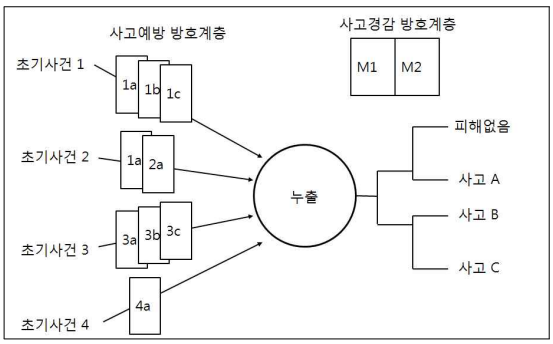
2. 방어선(Lines of Defence)/방호계층(Layers of Protection)의 개념

방어선 또는 방호계층이란 사고를 예방하거나, 경감시키는 독립적인 방어층으로 기존의 안전조치(Safeguard)와 다른 개념으로 적용된다. 예를 들어 방어선 또는 방호계층은 반응기의 원료 과잉 공급, 냉각실패와 같은 초기 사건이 반응기파열로 인한 위험물질의 누출과 같은 사고로 이어지는 것을 막거나, 사고의 심도를 경감시키는 역할을 한다. 아래의 그림은 이러한 방호계층 개념을 도식화한 것이다.



[그림 1] 방호계층

초기사건, LOD 또는 LOP와 같은 방호계층, 누출과 사고결과 사이의 관계는 다음의 그림과 같다.



[그림 2] 초기사건, 방호계층, 누출, 결과의 관계

[그림 2]와 같이 위험물의 누출은 수많은 초기사건에 의해서 발생할 수 있다. 그리고 각 초기사건에 대하여 누출을 예방하는 방호계층은 다를 수 있다. '초기사건 1'과 '초기사건 3'은 똑같이 위험물의 누출을 야기하지만 사건마다 누출을 예방하는 방호계층은 다르다. 반대로 '1a'와 같이 하나의 방호계층이 여러 가지 사건에 대해 적용되어질 수 있다. 일단 누출이 발생하면 사고경감 방호계층에 따라 그 피해의 범위는 다를 수 있다. 어떠한 사건/사고에 대해 특정한 방호계층이 어느 수준으로 설치되어 있는지를 파악하는 것은 위험을 관리하는데 중요한 요소가 된다.

3. LOP/LOD를 이용한 위험성평가기법

3.1 LOPA(Layer Of Protection Analysis, 방호계층분석)

LOPA는 방호계층을 이용하는 대표적인 위험성평가기법이다. LOPA는 일반적인 위험분석방법으로 확인된 시나리오를 평가하는데 사용된다. 따라서 LOPA는 일반적인 위험분석방법, 즉 정성적 위험성평가에서 도출된 시나리오 중 사고심도에 기초하여 추가적으로 분석이 필요한 위험한 시나리오를 선별하는 것부터 시작된다. 시나리오를 사고심도에 따라 구분하는 방법으로는 누출된 물질의 양에 따라 사고심도를 분류하거나, 사상자수, 사상가능한 지역의 범위 등 더욱 자세히 결과를 계산하여 분류하는 방법이 있다.

추가적으로 분석이 필요하다고 선별된 시나리오는 단일 초기사건-결과를 형성한다. 단일 위험에 대하여 분석될 수 있는 시나리오의 수는 이론적으로 무수히 많다. 예를 들어 [그림 2]를 보면 위험물의 누출이라는 단일 사고에 대해 총 16가지(4가지 초기사건 × 4가지 결과)가 도출되었다. 그러나 '피해없음'이라는 결과는 추가적으로 분석할 필요가 없으므로 총 12가지 시나리오로 선별되고, 이중 누출량이 적은 시나리오의 경우 분석할 필요가 없으므로 사고심도가 클 것으로 예측되는 시나리오로 최종 분석대상을 선별한다. 이렇게 선별된 시나리오는 사고로 이어지는 초기사건을 결정하는데 미국화학공정안전센터(Center for Chemical Process Safety)에서는 크게 3가지 형태(외부사건, 장치고장, 인적오

류)로 구분한다. '운전원의 훈련 부족', '불충분한 시험과 점검'은 초기사건이 아니며, 이것은 '인적오류', '장치고장'과 같은 초기사건의 잠재적인 원인이다. 이러한 근본적인 고장원인은 초기사건의 빈도에 영향을 미친다. 통계자료 등을 통해 초기사건의 빈도가 구해지면 가능한 환경조건의 확률이 배가되어 최종적인 초기사건 빈도가 결정된다. LOPA에 적용되어지는 빈도 및 사고가능한 환경조건은 단순화된 접근 방법을 사용하므로 높은 수준의 정확성을 보장할 수 없다. 따라서 복잡하거나 중대한 시나리오에 대해서는 정량적 위험성 평가기법을 사용하는 것이 바람직하다.

초기사건이 정의되면, 초기사건이 사고로 이어지는 것을 차단할 수 있는 독립방호계층(Independent Protective Layers, IPLs)이 분석되어져야 한다. 독립방호계층은 효과성, 독립성, 검증성의 조건을 만족시켜야만 인정된다. 즉, 독립방호계층은 설계대로 동작되면 사고를 예방하는데 효과적이고, 초기사건에 대해 다른 방호계층과 독립적이며, 사고예방 및 고장률 관점에서 효과성이 검증되어야만 인정한다. 따라서 모든 독립방호계층은 안전장치이나, 모든 안전장치가 독립방호계층이 될 수 있는 것은 아니다. 예를 들어 교육 및 훈련, 작업절차, 일반적인 검사 및 시험 등의 안전관리는 독립방호계층이 아니다. 독립방호계층의 조건을 만족한 방호계층에는 고장률이 입력된다. 여기에서 주의할 점은 사고예방 방호계층과 사고경감 방호계층의 차이이다. 사고예방 방호계층이 성공적으로 작동되면 초기사건이 사고로 이어지지 않지만, 사고경감 방호계층이 성공적으로 작동되면 사고가 발생하여도 사고의 피해크기가 작아지므로 허용할 수 있는 위험도를 가진 시나리오가 된다.

초기사건의 빈도에 각각의 독립방호계층의 고장률이 배가되면 시나리오에 관련된 사고의 빈도가 계산된다. 여기에 점화확률, 사고반경 안에 사람이 있을 확률, 사고에 노출된 사람이 사망할 확률 등이 고려되어 개인적인 위험이 결정되고, 여기에 노출된 사람의 수가 곱해지면 사고로부터 사망한 사람의 수가 예측된다.

이와 같이 사고의 위험도를 구하는 방법 이외에 심도분류, 최종빈도 등 수치에 의한 매트릭스 또는 표를 통해 사업장의 위험관리기준에 의해 의사결정에 사용될 수 있다. 허용할 수 없는 위험을 가진 시나리오에 대해서는 독립방호계층이 추가되거나, 독립방호계층의 고장률을 낮추어 재평가되어 안전도를 확보하게 된다.

3.2 TRAM(The Technical Risk Audit Method, 기술적 위험검사기법)

TRAM은 영국의 안전보건청(Health and Safety Executive)에서 위험한 중요사업장에 적용하기 위한 위험기반 검사기법으로 개발되었다. 현장검사 및 점검용 기법으로 만들어진 TRAM의 기본적인 접근방식은 시나리오를 정의하고 관련된 방호조치들을 확인한다는 점에서 LOPA의 접근방식과 유사하다. TRAM은 소프트웨어 패키지를 통해 수행되는데 분석자에 의해 사고 시퀀스, 초기사건의 빈도, 사고의 결과, 고장률이 입력되고, 소프트웨어는 허용할 수 있는 수준으로 시나리오의 위험도를 줄이는데 필요한 LOD의 수를 결정한다. 분석대상 시나리오의 LOD 수가 TRAM에 의해 필요하다고 예측되는 수를 초과하면 위험도는 합리적으로 판단하여 허용가능한 수준으로 판단된다. 반대로 TRAM에 의해

추가적인 LOD가 필요하다고 결정되면, 정량적 위험성평가와 같은 더욱 자세하고 추가적인 분석이 필요하다.

LOPA의 독립방호계층, 즉 IPL은 TRAM의 LOD의 개념에 대응된다. 그러나 TRAM의 LOD는 LOPA의 IPL보다 더 광범위하게 정의되어진다. IPL과 같이 LOD는 고장 시퀀스에서의 다른 LOD와 초기사건에 대해 독립적이어야 하지만, LOPA와는 달리 IPL 조건인 효과성과 검증성을 만족하지 못하는 자연적인 열 확산, 또는 추운 날씨와 같은 물리적인 조건이 LOD가 될 수 있다. 방어선의 등급이 결정되고 초기사건의 빈도로부터 빈도등급이 결정되어지면, 시나리오에 대한 심도등급이 주의깊게 선택되어져야한다. 심도등급은 허용여부를 판단하기 위하여 단순한 대수적인 과정을 사용하여 결정된다. 개인적인 위험의 허용여부는 관련된 모든 고장시퀀스로부터 나온 개인적 위험도를 합한 값과 허용가능한 기준값을 비교하여 결정된다. 고장시퀀스의 수를 예측하여 심도등급이 결정되어지고, 초기사건의 빈도등급과 필요한 LOD 등급의 합이 심도등급보다 크면 위험은 허용될 수 있다.

여기서 해당 시나리오에 주어진 심도등급은 적용되어진 위험허용기준에 따라 결정되는데, TRAM에는 심도등급의 표준분류가 제공된다. 자료로부터 결정된 실제 존재하는 LOD 등급과 필요한 LOD 등급의 차이가 양수이면 허용가능한 위험이 되고, 이 양수가 1과 같이 작은 수가 되면 심도 깊은 조사가 필요하다.

3.3 AVRIM2(Arbeidsveiligheidsrapport Inspectie Methodiek 2, 작업안전보고서 검사기법2)

AVRIM2는 독일 노무관리청을 위해 개발된 평가 및 조사기법이다. TRAM과 같이 AVRIM2는 위험성평가기법으로 개발된 것이 아니고, 운전원이 제출한 중요재해에 대한 현장안전보고서(Arbeidsveiligheidsrappoten 또는 AVRs)를 평가하는 검사원을 위해 개발된 기법이다. 이 기법으로 위험물의 누출을 예방하기 위해 설치된 LOD와 시스템을 평가하고 점검할 수 있다. AVRIM2가 LOPA와 TRAM과 다른 점은 방어선과 안전관리시스템 사이의 연결이다. AVRIM2에서 적절하지 못한 안전관리는 수많은 LOD의 실패를 야기하는 공통된 잠재적인 원인으로 간주된다.

이 기법은 검사원이 평가를 수행하는 데 필요한 많은 모듈로 구성되어있다. 첫 번째 모듈로 초기사건 매트릭스가 있다. 초기사건 매트릭스는 검사원이 잠재적인 사고와 관련된 모든 초기사건들이 고려되었는지를 확인할 수 있는 모듈이다. 두 번째 모듈은 초기사건 매트릭스에서 나타난 직접적인 사고원인에 대한 일반적인 결함수이다. 결함수의 목적은 누출과 관련된 모든 시나리오들이 고려되었는지를 확인하는 것이다. 다음 모듈은 위험도 매트릭스이다. 독일에서는 운전원이 다양한 사고시나리오와 관련된 위험을 평가하고, 그러한 결과를 위험기준과 비교하여야한다. 또한 운전원은 사용할 위험기준을 개발해야한다. 운전원은 일반적으로 준정량적 기법을 사용하는데, AVRIM2에서는 기준이 되는 위험도 매트릭스를 제공한다. 그리고 AVRIM2는 회사의 안전관리 시스템의 강점과 약점을 예측할 수 있는 모듈을 포함한다. 또, AVRIM2 내에 포함된 제어와 감시회로는 검사원이

운전원의 안전관리 시스템을 평가하는데 유용한 모델이다.

LOPA는 안전관리 문제를 특별히 다루지 않으므로 안전검사와 점검과 같은 다른 방법과 상호보완이 될 수 있다. LOPA 분석의 결과는 특정 방호계층을 설치하고, 관리하고, 시험하고, 점검하는 것을 강조하기 위해 사용될 수 있으며, AVRIM2와 같은 검사 프로그램은 이러한 활동이 적절히 수행되어지는 지를 증명하기 위해 사용될 수 있다.

3.4 PLANOP(Protection Layer Analysis and Optimisation, 방호층분석 및 최적화)

PLANOP은 벨기에 노동부의 화학위험본부에 의해 화학공장의 방호층에 대한 정성적 분석을 위해 개발된 기법이다. 이 기법은 기존의 설비에 대한 연구를 위해 사용될 수 있을 뿐만 아니라, 진보적인 공정설계를 위해 사용될 수 있다. 또한 안전대책의 시행에 대한 결정을 위해서 공정위험과 관련된 정보의 분석, 수집, 조직을 위해 필요한 기법이다.

먼저 PLANOP은 '피해원(damage sources)'와 '사고원(event sources)'의 두가지 모듈로 구분된다. 피해원은 위험의 존재하는 근본적인 원인으로, 다시 위험물과 반응의 두가지로 구분된다. 사고원은 누출의 원인에 대한 것으로 기본적으로 과압에 의한 누출, 손상에 의한 누출, 인적오류에 의한 누출, 공정상 개구부를 통한 누출로 구분된다. PLANOP은 또한 두 그룹의 방호계층, 즉 누출전 예방 방호층과 누출후 경감 방호층으로 구분된다. 그러나 비상계획은 PLANOP 범위 밖 안전조치이다. 즉, PLANOP은 사고원과 피해원, 그리고 방호층의 분석을 통해 위험경감대책을 제시한다.

PLANOP은 방호층에 대한 분석을 위한 기법으로서 정밀한 위험분석이 필요하지 않은 상황에서는 유용하며 정밀한 평가를 수행하는데 충분하지 못한 기법이다. 최근 PLANOP은 LOPA 기법과 같이 사용하여 보완적으로 수행되고 있다.

3.5 Safety-Barrier Diagrams(안전방호벽도형기법)

Safety-Barrier Diagrams은 LOPA와 TRAM과 같이 LOP/LOD를 고려한 기법이다. 도형으로 된 초기사건, 방호벽, 결과의 표현은 시스템의 고장 논리를 이해하는 데 유용하다. 방호벽은 TRAM의 LOD가 그렇듯이 LOPA의 IPL보다 광범위하게 정의된다. 예를 들어, 환경적 방호벽은 피해를 경감시킬 수 있는 바람의 방향과 같은 환경을 포함한다. 방호벽의 점수를 결정하기 위한 기준은 LOPA에 적용되는 원칙, 즉 사고결과의 수준에 따라 필요한 IPL의 수가 결정된다는 점에서 유사하다.

Safety-Barrier Diagrams은 다양한 방호벽의 역할과 시스템의 고장에 대한 유용하고 도식화된 표현을 제공한다. 그러나 고장논리가 복잡한 상황, 그리고 일반모드의 고장가능성을 있는 상황에서 Safety-Barrier Diagrams를 적용하는 것은 적절하지 않다. 그리고 결함수분석과 같은 정교한 기법이 적용되어야하는 상황에서도 적합하지 않다. 또한 현재의 Safety-Barrier Diagrams는 위험을 정확히 계산할 수 없다. 추가된 방호벽의 점수로는 추가된 위험경감조치의 이점을 쉽게 평가할 수 없으므로 방호벽의 추가가 위험을 합리적으

로 허용가능한 영역으로 낮출 수 있는지 판단하기 어렵다. 이러한 단점은 방호벽의 점수 대신 도형에 고장률을 사용하는 기법으로 보완하여 극복될 수 있다. 결과의 빈도는 도형을 통해 적절한 경로를 따라가며 각 방호벽의 고장률을 초기사건의 빈도에 배가하여 얻어질 수 있다.

4. 결론

위험성을 평가하는 방법으로는 단순하고 정성적인 기법부터 정밀하고, 정량화된 기법까지 다양한 기법이 존재한다. 모든 위험성평가는 위험을 분석하고 예방과 경감조치들로 인해 합리적으로 판단하여 허용가능한 위험수준(ALARP, As Low As Reasonably Practicable)을 만들기 위한 것이다. 위에 소개한 LOPA, TRAM, AVRIM2, PLANOP, 그리고 Safety Barrier Diagrams와 같은 위험성평가기법은 LOD 또는 LOP를 이용하여 사업장의 위험을 새로운 측면에서 분석하고 합리적인 위험수준을 관리하는데 도움이 될 수 있다. 위험성평가기법의 장단점을 보다 정확히 파악하고, 적용할 때 효과적이고 효율적인 안전관리가 이루어질 것이다.

작성 : 방재컨설팅팀 최승호