플랜트의 安全確保에서 人間活動의 重要性

지난 6月8日부터 10日까지 英國 Blackpool에서는 (TMI와 체르노빌事故 以後) 原子力安全을 위한 國際的인 어프로치를 주제로 세미나가 개최되었다. 다음은 이 세미나에서 英國原子力公社(UK-AEA)의 Nigel Holloway氏가 발표한 內容이다.

有史 이래로 인간의 실수로 인한 사고와 이에 의한 사상자들이 많았었다. 역사상 모든 事故死의 근본적인 원인을 분석해 보면 대부분의 사고들이 인간의 실수로 인한 것이었다. 이는 그다지 놀라운 사실이 아니다. 사고의 유형은 자동차가 순간적으로 미끄러져서 승객 한명이 사망하는 경우에서부터 수백만의 죽음을 초래할 수 있는 군사, 정치, 공중보건상의 실수까지 광범위하다.

실수를 방지할 수 있는 능력을 함양하기 위한 교육과 기술에는 많은 진보가 이루어졌으나, 동시에 사고가 발생했을 때 있을 수 있는 파괴력의 정도도 더욱 심각해졌다. 인간의 실수로 인한 모든 재해에서 차지하는 비중이 그다지 크지 않았음에도 불구하고 거대한 産業設備의 稼動은 분석과 논쟁의 주안점이 되어 왔다. 이는 현대기술의 특성상 인간실수 방지기능이 증진되더라도 일단 실수가 발생했을 경우 그 결과가 매우 심각해지기 때문이다.

산업설비의 안전성을 확보함에 있어서 기기의 품질보증과 정교한 계통구성을 주된 방법으로 채택하고 있다. 계통구성에 있어서 多重性, 多樣性을 부여하여 많은 부품들이 모여서 구성된 계통내의 불가피한 無作爲 故障(Random Failure)의 파급 효과를 방지하고 있다. 이러한 안전성확보 방법들은 매우 성공적으로 활용되어 왔으며, 따라서 현대의 복잡하고 거대한 산업시설들이 산업화 초기의 간단한 기계(예 : 증기기관)들 보다 사고의 빈도가 훨씬 적다.

그러나 기계나 계통설계에 적용되는 분석기법이나 품질관리기법이 인간설계를 위해 轉用될 수는 없다. 이제까지 교육과 훈련이 기술적으로 안전한 인간의 양성에 一助는 해 왔으나 우리가 기계에 대해 이룬것을 인간에 대해서도 이룬다는 것은 불가능하며, 또 우리가 이를 원하는 것도 아니다. 따라서 우리의 분석능력과 제어능력 밖에 없는 人間要素들을 항상 고려해야 한다. 과거의 경험을 조사, 분석하여 인간요소에 대한 지식과 인간요소를 좋은 방향으로 지속적으로 활용할 수 있는 능력을 습득해야 한다. 그러나 이러한 점에도 불구하고 인간실수는 과거와 마찬가지로 미래에 있어서도 중요성을 지니게 될 것이다.

이러한 점들을 염두에 두고 설계에서 고려되지 않았던 사고에 대해 인간요소가 어떻게 작용했는가를 역사상의 네가지 사고를 사례로 하

여 살펴 보고자 한다.

Flixborough 事故

평소 적절한 설계와 성능을 지녔던 설비를 수년간 운전한 후 보수를 하고 설계개선조치를 취했다. 그러나 원래 설계에 적용되었던 품질 보증요건이 보수, 개선시에 적용되지 않았기 때문에 교체부품에 심각한 설계상의 하자가 있었다. 이러한 상황에서 재가동하자 設備의 일부가 견디지 못해 파괴되었다.

TMI 事故

원자로계통에서 비교적 사소한 고장이 발생하자 자동안전조치가 취해졌으며, 이 조치는 급수계통의 동시작동불능에도 불구하고 충분한 대처가 가능토록 되어 있었다. 그러나 운전원의 판단 실수로 자동안전 기능을 정지시켰으며, 이로 인해 노심냉각불능상태에서 노심의 부분 용융이 발생했다.

즉, 사고진단이 어려운 상황에서 사태가 확대되었으며 운전과 안전상의 일부 관리 소홀로 인해서 사고가 야기된 것이다. 안전성 관련 운전절차를 사전에 점검했었더라면 자동안전장치를 운전원이 정지시킬 수 있는 매우 위험한 가능성은 사전에 발견, 배제될 수 있었을 것이다.

Bhopal 事故

메틸 · 아이소시아네이트를 대량 취급할 경우 냉동장치, 걸름장치(Scrubber) 등을 포함한 일련의 조치를 통해 안전성이 유지되어야 한다. 만약 이러한 방법들을 준수하여 운전을 했거나 (또는 운전이 가능했다면) 어지간한 사고의 경우에는 독극물의 배출이 없이 공장이 견디어 나갈 수 있었을 것이다. 그러나 부적절하고 위험한 工程으로 인하여 모든 안전조치가 無用化되었고 경미한 사고로 인해 많은 독극물이 所外로 유출되었다. 다른 세가지 사고들과는 대조적으로 同 사고는 설비 자체에는 아무런 위해도 주지 않았다. 그러나 인근 주민에 대한 결과는 비참한 것이었다. 즉, 이 공장에서는 시설보호와 대중보호를 극히 비정상적으로 별개의 차원에서 취급하고 있었으며, 결과적으로 대중에게 큰 불행을 안겨 주었다.

체르노빌 事故

원자로의 설계는 운전원이 反應度와 출력의 제한치를 엄격히 준수함을 전제로 하여 이루어진다. 따라서 만약 이러한 前提가 무시되면 원자로는 불안전한 상태가 된다. 체르노빌사고는 당초의 계획에 어긋나게 어떤 실험을 수행한 결과 반응도 제한치를 초과하여 인허가상 금지되고 있는 불안정한 상태로 원자로가 폭주한 결과이다.

즉, 사소한 절차위반으로 인해 원자로의 출력이 급격히 제어불능상태로 증가되었으며, 원자로가 극심하게 파괴된 것이다. 이 사고를 검토해 보면 체르노빌 발전소의 그 어느 누구도 "날벼락"의 가능성에 대처하지 않았었음을 알 수 있다. 문제의 근원은 사고발생 이전에 常存하고 있었으며, 사고 후의 대처방안 또한 수립되어 있지 않았다.

이러한 사고들 중에 TMI사고 만이 불가능하지만을 않았겠지만 사고발생 이전에는 예측이 어려운 일련의 행위들로 인한 것이었다. 다른 사고들은 모두 최종 결말 이전에 이미 시설의 운영상태가 정상에서 이탈되었었다. 앞에서 분석한 사고들을 볼 때 사고방지를 위한 원칙적인 조치들이 사전에 가능했음은 매우 고무적이라고 할 수 있다. 만약 이러한 사고의 주된 요인들이 부적절한 조건에서의 운전이었다면 시설감시 및 적절한 對應節次에 따라 사고를 미연에 방지할 수 있었을 것이다. 물론 항상 완전한 상태에서 운전되지는 않음을 인정해야 한다. 그러나 합리적인 제한치 범위내에서 정상운전이 가능하며 앞에서 언급한 사고에서 처럼 엄청난 정상상태 이탈은 방지할 수 있다.

그러나 TMI사고와 같이 사고원인 발생 후

(Post－Incident)의 실수에 대해서 어떠한 대책이 마련되어야 하는가는 그다지 명확하지 않다. 이러한 실수들은 사고발생 이전에는 명확하게 발전될 수가 없다.

순간적인 실수는 고정되고 예측가능한 시스템구조(Framework)내에서 발생하므로 문제점을 事前에 연구한다면 문제해결에 더욱 접근할 수 있다. 만약 이러한 연구가 없다면 비교적 간단한 설비에서도 인간의 상상력을 초월한 실수에 직면하게 되는데 이는 매우 두려운 문제이다.

1. 가장 重要한 行爲

이제까지 주요사고를 검토하고 이에 대해 논의해 보았다. 그 결과 인간실수로 인한 시설의 안전성 상실을 방지하기 위해 우선적으로 해결해야할 점이 있음을 알았다.

인간실수로 인하여 안전범위 밖으로 플랜트의 상태가 이탈되더라도 그 실수 자체로는 사고로 까지 진행될 수는 없으며, 단지 과도상태와 예측불허의 상황을 초래하게 된다. 따라서 이러한 정상상태로 부터의 이탈 방지에 우선순위를 두어야 한다. 이는 비상시 처럼 순간적이며 예상 밖의 행위를 다루는 것이 아니고 비교적 느리고 관찰가능한 일들을 다루기 때문에 원칙적으로는 다소 용이한 과제이다.

사고원인 발생후의 인간실수는 계통상태가 알려진 시설에서 발생할 경우가 안전상태로 부터의 심각한 이탈이 예상되는 시설에서 발생할 경우 보다 그 예측 및 시정조치가 용이하다. 후자의 경우 未知의 인간실수구조(Framework)가 형성되기 때문이다. 시설의 상태에 대한 예측이 가능하고 또한 합리적으로 상태범위를 축소시킬 수 있다면 사고원인 발생후 인간실수를 야기하는 혼란을 감소시킬 수 있다.

부적절한 운전상태를 야기시킬 수 있는 인간실수는 여러분야에 걸쳐서 존재한다. 앞에서 설명한 네가지 사고들은 다음과 같은 실수로 인한 것이었다.

○ 설계상의 하자(체르노빌)

○ 부적절한 시설운전(체르노빌)

○ 플랜트 개조에 있어서의 품질보증 결여(Flixborough)

○ 부적절한 프로세스 관리 및 위험에 대한 경각심 결여(Bhopal)

○ 운전상태의 부적절한 제어 및 관리(TMI)

비록 앞의 사례들로 부터 단 한가지의 기술적 문제를 인간실수에 있어서 가장 중요한 원인으로 집어 내기는 불가능하다. 효과적인 운전 제어 및 사고방지 대책은 궁극적으로는 시절의 관리기능에 달려있는 것으로 나타나고 있다. 이러한 관점에서 볼 때 인간실수로 인한 다양한 위험들을 감시, 제어하는 방법과 동기들이 유발될 수 있다. 적절한 관리가 되지 않는 상황에서는 시설을 위험한 상태로 진전시킬 수 있는 여러가지 인간실수가 존재할 수 있는 것이다. 따라서 시설의 운영관리에 있어서 플랜트의 안전에 영향을 미치는 가장 중요한 인자는 인간의 행위임을 명심하여야한다.

2. 人間실수의 對處

인간 마음속에 내재한 실수의 근본적인 원인을 제거할 수 없는 상황에서 일단 발생한 실수의 처리에 중점을 두어야 한다. 인간실수는 크게 두가지로 분류되고 있다. 하나는 사고원인 발생전(pre-event 또는 pre-meditated) 실수로서 부적절한 운전 상태를 유발시키는 것이고, 다른 하나는 사고발생후(post-event, non-pre-meditated) 실수로서 부적절한 대응을 유발시키는 것이다. 비록 방식은 틀리나 두가지 유형 모두 예측(Anticipation), 감지(Feedback), 시정(Correction)으 순서에 따라 해결이 가능하다.

가. 실수에 대한 對處

인간실수 처리에 있어서 처음 단계이면서도 가장 중요한 단계는 실수가 발생할 수 있음을


▲Flixborough 事故現場

알아내는 것이다.

이러한 과정을 통해서 설비운전에 있어서의 거의 모든 실수가 즉각 배제될 수 있다(기기의 무작위적인 고장상태 발생과 같은 형태와 빈도의 기기작동 불능상태를 초래하는 운전조치도 이 실수에 포함된다). 이러한 종류의 실수는 기기의 무작위적인 고장을 시설설계 과정에서 이미 반영되어 있어야 한다. 또, 각 기기의 고장이 있더라도 인간실수가 특별히 크게 작용하지 않는 한 이제까지의 설계는 계속 효과적일 것이다.

따라서 반드시 예측되어야만 하는 重要한 실수는 단순한 운전상의 실수가 아니라 그 특성이 더욱 구조적인 실수들이다. 이 실수들은 시설의 상태를 정상상태로 부터 또는 어떤 조치를 통해 의도했던 상태로 부터 심각하게 이탈시킬 수가 있다. 이러한 종류의 실수를 예측함에 있어서는 다음과 사항들이 고려되어야 한다.

○ 실수가 영향을 미치는 안전성관련 분야의 식별 방법.

○ 실수의 발생을 차단하는 방법.

○ 실수가 발생했으면 이를 감지해 내는 방법.

○ 실수를 알았으면 이를 시정하는 방법.

이상의 어떠한 방법도 실수가 발생할 때마다 즉각 확립될 수는 없으며, 시설의 전 수명 기간을 통해 적용될 수 있도록 사전에 확립되고 실행되어야 한다. 이러한 방법의 확립 자체는 기술적인 사항이지만 모든 상위관리 조직에 의해서 감독되어야 가능하다.

실수가 영향을 미치는 분야의 판단여부는 여러가지 종류의 시설분석기법을 활용하면 가능하다. 이 기법들 중 가장 잘 알려진 것은 확률론적 위험도평가(PRA)이다. 이는 여러가지 조합의 형태로 안전기능의 작동이 실패했을 때 어떠한 결과가 발생하는가를 평가하며, 따라서 해당 기능의 중요도를 평가할 수 있다. 그러나 실수 자체가 단일사고기준(Single Failure Criteria) 과 같은 결정론적인 기준을 위반하게 되는 경우에는 결정론적 위험평가기법이 이용될 수 있다.

실수의 발생을 차단하는 방법은 품질보증계획에 이미 반영되어 있다. 그러나 이러한 품질보증계획이 전술한 몇몇 사고설비에서는 시운전 이후에는 이행되지 않았다. 결과적으로 설계나 운전상의 개선에 있어서 실수가 개재되었는데 이는 설계, 건설단계에서와 같은 품질보증절차를 지속적으로 이행하였으면 초기에 방지가 가능했었을 것이다.

실수가 영향을 주는 분야의 식별 및 그 분야 관련 활동에 대한 품질보증 계획의 실천과 같은 예측적인 성격의 활동들은 설비안전에 영향을 미칠 수 있는 많은 실수들을 초기에 더 이상 진행되기 이전에 차단시킬 수 있다. 이러한 활동들은 장기적인 사전계획을 필요로 한다. 그러나 몇몇 실수들은 예측을 피해가거나 또는 운전초기에 발생된다. 이러한 실수들은 감지(Feed back)와 제어를 통해 처리되어야 한다. 비록 설비운전이 단기적인 목표에 최상의 가치를 둔다 할지라도 이러한 방법의 확립은 장기계획 하에서 용이함은 물론이다.

나. 실수의 感知

前述한 분석, 식별, 품질보증의 망을 피해서

발생했거나 시설운전 초기에 발생하는 인간실수들은 일단 발생하면 이를 감지할 수 있어야 한다. 실수로 인하여 안전상태에서 벗어는 났지만 안전기능의 작동을 초래하는 사고로는 아직 진전되지 않았을 경우 같은 상황이 재발될 수 있는 시간 이내에 효과적인 실수의 감지가 이루어져야 한다. 상황 사이의 시간 간격이 수일 미만인 경우는 거의 없다. 따라서 조직적인 검사 및 감시계통으로의 자료입력을 통해서 설비상태의 감시가 매우 효과적으로 수행될 수 있다. 반면에 사고원인 발생후의 실수나 순간적 실수는 전술한 경우 보다 짧은 시간내에 감지가 이루어져야 한다. 이에 필요한 시간은 수초내지 수일로서 사고원인 발생전의 시설감시 경우와는 분석 및 자료입력시스템이 전혀 다르다.

모든 관련 變數들에 대한 상태를 주기적으로 조사하고 관리자에게 보고를 하는 경우 시설의 안전상태 감시는 여러 가지 방법으로 수행될 수 있다.

최근에 와서 설비감사컴퓨터가 개발되었는데 확률론적기법을 이용한 사고해석이 가능하며, 해석결과를 관련 시설에서 조사한 현재의 상태와 비교할 수 있다. 아직 이 감시기는 인간실수로 인한 취약점이 신중하게 연구된 후에야 도출이 가능할 모든 안전성관련 사항들을 반영할 수는 없으나, 이러한 발상 자체는 부적절한 안전상태의 발생을 막기 위한 온라인감시체제의 필요성을 시설관리자들이 명확히 인식했음을 시사하는 것이다.

사고원인 발생후 실수와 관련된 상태의 감시는 사고원인, 발생전의 상태감시 보다 어려운 과제이다. 즉, 많은 경우에 있어서 시간이 매우 제한되어 있기 때문이다. 그러나 일단 사고원인 발생 후의 실수로 인해서 안전조치를 소홀히 하게 되면 관련자가 실수를 보고하거나 최소한 시정조치의 필요성도 보고하지 않을 경우 시정조치가 취해질 가능성은 매우 희박하므로 이러한 감지기능은 매우 절실하다. 효과적인 감지를 위해서는 운전자가 이에 관심을 기울이고 있어야 하고, 시설의 변수를 운전원이 숙지하고 있는 시설모형과 잘 일치시켜야 한다. 또한 가장 중요한 문제점은 인지하고 적절한 해결책을 선택함에 있어서 도움을 줄 수 있도록 가능한 모든 사고결과를 고려한 우선대처 순위를 부여해야 한다는 것이다. 그러나 이는 계측장치 및 인간공학적 설계의 관점에서 아직 힘든 분야이고 또한 컴퓨터의 사고判斷(Interpretation) 기능과 진단기능 역시 좀 더 정립되어야 한다. 더군다나 감지의 적절성은 각 상황별 특성에 맞게 평가되어야 한다. 사고의 원인 발생시 상태를 감지하고 시정조치를 수행함이 어렵다는 것은 이직은 이 작업이 인간실수에 대처하기 위한 次善의 방법이며, 우선적인 대처방법은 설비의 상태를 사고원인 발생 이전에 정상상태로 환원시키는 것이다. 실수가 유발될 경우 매우 신속한 감지조치가 이루어져야 한다. 그러나 시정조치는 계통설계 자체와 비해볼 때 매우 제한적이다. 그럼에도 불구하고 이러한 제약 조건들이 아주 심하지 않을 경우에는 실수장치 즉 차선의 대응책이 절실히 요구된다.

다. 실수의 解決

이 단계는 원리상으로는 가장 간단하다. 즉, 사고원인 발생후의 조치에 있어서 실수가 일단 식별만 되면 자연적으로 해결될 수 있다. 실수의 해결을 위한 조치는 모든 프로세스중 가장 중요하다. 시정조치는 일반적으로 정상이탈을 바로잡기 위한 운전절차, 보수절차의 수행, 또는 사고원인 발생후의 실수를 시정하기 위한 비상운전절차 수행을 통해 이루어진다.

절차서에 의한 수정조치는 인간실수로 부터의 방호 이외에 부수적으로 무작위적 기기고장으로 부터의 방호도 가능하게 한다.

앞에서 논의한 모든 절차서의 내용 그 자체는 모두 전문성을 띄고 있다. 그러나 안전프로그램에 있어서 이러한 조치를 실행하는 책임은 관리자에게 있다.

라. 실수의 分析

인간실수의 처리는 어떤 일이 왜 효과적인가 또는 얼마나 효과적인가 보다 무엇이 효과적인가에 주안점을 두는 노력이라고 할 수 있다. 이러한 경향이 인간실수처리에 있어서 어떤 발전을 추구하는 것을 방해하지는 않으나, 이 경우 방향성과 효율성이 분명히 결여된다. 앞에서 언급한 인간실수를 적용하고 분석하기 위해서 갖고있는 능력을 시정조치와 사고원인 발생 전의 상태감시에 있어서는 '우수', 실수의 식별과 예방적 품질보증에서는 '양호', 사고원인 발생 후의 실수의 감지 및 처리에 있어서는 '불량'이라고 평가할 수 있다. 사고원인 발생 후의 감지, 시정이 차선이고 사고원인 발생 전의 설비상태 유지가 우선이므로 이러한 평가가 그다지 틀린 것은 아니다. 그러나 현재로서는 관리 행위의 효율성과 시설의 안전성에 지대한 영향을 줄 수 있는 관리상의 인간실수를 분석할 수 있는 기법이 거의 없고, 기술적 관점에서 본 인간실수의 처리과정이 관리측면과는 전혀 별개임을 감안한다면 불만족스런 상황이 노출되고 있다. 즉, 시설의 안전성에 있어서 인간실수가 중요함을 감안한다면 관리기능의 분석능력이 현재 결여되어 있음에 관심을 두어야만 한다. 다른 분야의 인간관리 활동들도 마찬가지로 분석이 용이하지는 않다. 그러나 원자력 및 대규모 산업시설의 경우 이제까지는 안전성 관점에서 체계적, 분석적 접근을 많이 시도해 왔다. 따라서 이들이 관리측면에서도 같은 역할을 수행할 수 있으리라고 기대된다.

3. 機器故障과 人間실수의 유사성

원자력개발 초창기에 안전관련 설계자 및 분석자들은 기기의 고장이 초래할 수 있는 심각한 사고의 가능성을 극복해야 했었다. 원자로 운전경험을 통해서 얻은 기기의 신뢰도자료를 이용하는 현재의 확률론적 분석기법은 당시에는 존재하지 않았었다. 원자력 초창기의 무작위적인 기기고장문제는 고장이 원자로계통 내에서 예측불허였고 관련자료가 없었다는 점에서 현재 우리가 직면하고 있는 인간실수문제와 많은 유사점을 지니고 있었다고 할 수 있다. 기기고장문제는 원자로의 안전성 확보를 위해 현재도 채택하고 있는 결정론적 안전분석기법을 이용하여 해결되기 시작했다. 근래에 와서는 확률론적 기법이 결정론적인 기법을 보완하고 있으므로 사고의 확대억제와 효과적인 사고방지가 가능하게 되었다.

결정론적 기법에서 인간실수 요소를 배제한 결과 원자로계통은 인간실수에 대해 매우 취약하게 되었다. 이와는 대조적으로 일반 産業部에서는 거의 고려하지 않은 무작위 기기고장을 많이 고려하고 있다.

그런데 결정론적 기법은 명백하게 인지할 수 있는 고장에 대해서는 매우 효과적이었으므로 인간실수문제들의 적용도 고려할 수 있다.

가. 결정론적 事故解析

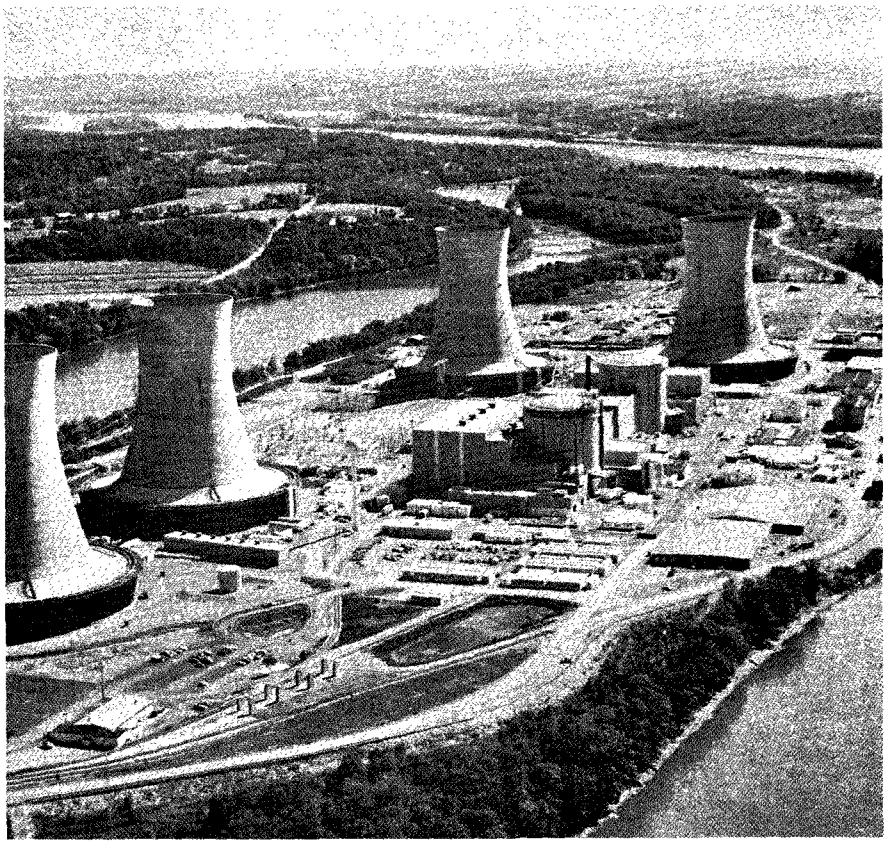
결정론적 사고해석은 미국 NRC의 규제지침 1.70 및 표준검토 절차(SRP), 경수로형 발전소 FSAR의 사고해석 부분으로 대표될 수 있다. 이는,

1) 여러 종류의 보수적인 초기事象(예 : 대구경 배관 파단)들을 정의하고,

2) 각 사상에 있어서 안전계통의 작동불능형태를 정의하고(예 : 능동기기 한개의 작동불능과 所外電力供給中斷),

3) 보수적인 모델을 이용하여 작동이 가능한 안전계통에 의해 미리 설정된 어떤 운전제한치가 초과되지 않음을 입증한다(예 : 핵연료피복재 온도 1,204℃미만).

이러한 접근방식은 만약에 계통이 한 부류의 사고에 견딜 수 있다면 같은 부류의 소규모 사고의 경우에는 더욱 쉽게 견딜 수 있으므로 사고해석도 필요없다는 개념에 기초하고 있다. 즉, 기기고장의 경우만을 다룬 결과 논리적 타당성이 부족함에도 이러한 개념이 창출된 것이



▶Three Mile Island原子力發電所 全景

다. 결정론적 접근방식은 이의 간단한 개념과 기법의 명료성으로 인해 현재는 이러한 장점이 약점도 될 수 있음이 드러났지만, 원자력산업계에서 광범위하게 인정받아 왔다. 그렇다면 이러한 단순한 접근방식이 인간실수 문제에도 적용될 수 있는가를 특히 관리측면에도 적용될 수 있는가를 살펴보아야 한다.

관리측면을 포함한 인간실수 취급에 대한 결정론적 접근은 기기의 고장 처리에 대한 접근과 유사할 수 있다. 즉 여러가지 실수를 가정하고 발전소의 계통이나 운전원이 실수를 극복하여 사고결과를 설정치내로 제한시킬 수 있음을 보인다. 기기고장의 경우와 마찬가지로 인간실수의 모든 가능성을 파악하기란 불가능할 것이나 몇몇 심각한 실수의 경우에는 이 기법으로 확실하게(비록 입증은 어렵더라도) 대처할 수 있음은 매우 고무적이라고 할 수 있다.

결정론적 접근방법으로 원전에서의 중대인간 실수를 처리하는 과정을 몇몇 사례를 들어 제시했다. 다음의 사례들은 전술한 여러 부류의 실수들을 다루고 있다. 실제 분석에 있어서는 더 복잡한 해석을 요구하는 경우가 많을 것이다.

나. 補修 및 發電所狀態

1) 가정된 실수

보조급수계통이 부실하게 보수되어 격리밸브들의 개폐상태가 정상이 아니었고, 따라서 정상운전중 보조급수계통의 작동이 불가능했다.

2) 결정론적 요건

이러한 실수는 반드시 운전개시 이전에 점검절차에 의해 발견, 시정되어야 하고, 이는 보수요원이 아닌 다른 요원들이 수행해야 한다.

3) 분석

발전소내의 보수책임부서는 이들의 절차서가 모든 보수작업후 독립된 점검 작업을 수행토록 규정하고 있음을 입증해야 한다.

4) 시험

규제기관 또는 자체검사요원은 보수작업 후에 일부러 실수상태를 만들어 놓고 점검절차에 의해 실수를 감지할 수 있는가를 시험할 수 있다(물론 운전개시 이전에 이 사실을 알려야 함).

다. 事故原因 발생후의 運轉員 실수

1) 가정된 실수

원자로 긴급정지 후 운전원이 무슨 이유에서인지 모든 보조급수계통의 기능을 정지시켰다.

2) 결정론적 요건

운전원은 실수 이후의 노심냉각상태를 정확히 진단할 수 있어야 하고, 일차계통의 방출밸브가 열리기 이전에 노심냉각을 재개시킬 수 있는 절차를 알아야 한다. 중앙 제어실내의 계기는 부정확한 지시를 할 수도 있다.

3) 분석

실수 이후의 노심냉각상태를 분석하여 운전원에게 노심냉각 불량상황을 경고할 수 있어야 하며, 복구를 위한 절차서는 방출밸브 개방 이전에 유전원이 이용할 수 있어야 한다.

4) 시험

모든 접근방식과 분석방법을 시뮬레이터를 통해 시험이 가능하다.

라. 運轉管理上의 실수

1) 가정된 실수

안전성과 관계없는 기능 F를 개선하기 위해 (경제성 증진, 실험 등을 목적으로) 운전원이 표준안전절차서를 무시 또는 개정하기로 하였다. 이는 기술지침을 위반할 가능성이 있다.

2) 결정론적 요건

이러한 사항은 반드시 기능 F와 안전성확보를 모두 책임질 수 있는 관리자에게 보고되어야 하고 절차서가 시행되기 이전에 관리층은

> **産業設備의 安全性을 확보함에 있어서는 機器의 품질보증과 정교한 계통구성을 그 방도로 채택하고 있으며, 이러한 안전성 확보방법들은 성공적으로 활용되어 현대의 거대한 산업시설들이 初期의 단순한 기계들보다 사고의 빈도가 훨씬 적다.**

결정사항을 운전원에게 회신해야 한다. 만약 절차가 중요한 운전지침을 위반할 수 있을 경우, 이는 반드시 운전원에게 통보되어야 하고 절차의 시행을 적절한 검토가 완료될 때까지 보류되어야 한다.

3) 분석

분석의 주안점은 운전원과 관리층 사이의 의사전달의 속도이다. 이 속도에 의해 안전성과 관계없는 기능을 개선하기 위해 개정된 절차의 무단시행 가능성을 排除할 수 있다. 이러한 개념이 사고를 제어하기 위한 운전원의 재량권을 간섭하는 것은 아니다.

4) 시험

이러한 상황은 모의훈련에 의해 시험할 수 있다. 圖上혹은 시뮬레이터를 통해 특정한 상황을 만들고 운전원과 관리층은 實時間에 이를 처리한다.

비록 앞에서 예시한 세가지 경우들이 현실에서는 좀처럼 나타나지 않는 상황들을 다루기 있음이 조금은 어색하지만 이 사례들은 안전성 확보를 위해 계측제어 시스템의 이제까지의 접근방식과 아주 유사하다. 계측제어기기들은 플랜트 상황을 감지하고 논리회로에 정보를 전송하며 안전기기에 명령을 내린다. 인간관리란 인간 사이에서 이와 같이 비슷한 과정을 수행하는 것이다. 따라서 계속 제어기기와 비슷한 분석기법과 확인기법을 적용함에 무리가 없다. 이러한 접근방식은 아주 명확하고 자세한 성공 또는 실패의 사례를 제공할 수 있으며, 운전원

과 관리자의 자질평가에도 도움을 줄 수 있다.

원자력안전에 있어서 인간관리에 대해 아주 면밀한 조사와 시험을 필요로 하는 분야는 원전비상연습니다. 즉 模擬된 비상사태에 대처한 관리구조, 의사소통, 결정능력, 실행능력들을 규제요건과 비교하고 시정조치를 취하게 된다. 따라서 이러한 개념을 관리분야까지 확장하여 실제 비상상황이 전개되기 이전에 사고를 방지할 수 있도록 대비하는 것이 매우 논리적이라 할 수 있다. 또한 發電所 관리조직의 비상상황 방지능력을 평소에 시험하는 것이 훨씬 쉽다. 왜냐 하면 비상연습시에 필요한 긴급대응 조직들이 이 경우에는 불필요하기 때문이다.

마. 確率論的 위험도 평가

결정론적 기법이 지배하던 원전 안전해석분야에 확률론적 위험도 평가기법의 도입은 기존의 결정론적 구조 속에서는 쉽게 얻을 수 없었던 다음과 같은 중요한 이익을 주고 있다.

1) 결정론적 해석이 가지고 있던 보수성의 정량화 및 예시와 이의 의미

2) 결정론적 해석에서 고려하지 않았던 주요 동시고장(Multiple Failure)의 가능성

3) 결정론적 해석에서는 고려하지 않았던 실제적 또는 잠재적인 사고에 있어서의 사고결과의 개별평가 및 強度에 따른 방호대책 우선순위의 결정

확률론적 분석기법을 인간실수처리에 적용할 경우 비록 첫번째 사항은 실효성이 거의 없으나 나머지 두사항에 대해서는 매우 유용하다. 즉, 동시고장 가능성을 파악해 내고 事故結果의 강도를 각기 파악해 낼 수 있음은 결정론적 분석을 함에 있어 적절한 요건설정 지침으로 활용할 수 있다.

인간실수의 확률론적 계량화는 아직은 힘이 들지만 방호조치를 요구하는 중대한 실수와 방호조치의 필요성이 없는 실수를 개략적으로 분류함에는 적합하다고 볼 수 있다.

운전조직이 확률론적 위험도분석을 응용하게 발전소운전 관리자가 사고대책 수립기능을 충실히 수행할 수 있게끔 경각심과 동기를 유발시킨다.

4. 結　論

지금까지 네가지 주요 설비사고를 조사하고 이를 고찰한 결과 가장 중요한 인간실수의 유형은 사고가 발생하게끔 설비를 정상상태로 부터 이탈시키는 실수이다. 적절한 설비운영 상태의 유지는 조직내의 많은 업무기능간의 협조를 필요로 하고 이를 명확히 하기 위한 책임소재는 관리기능에 있다.

두번째로 중요한 인간실수의 유형은 TMI사고 처럼 사고원인 발생후의 운전에 있어서의 운전원이 확신을 갖고 범하는 실수이다 이러한 실수는 설비의 운영상태가 부실하게 되며, 그 파급효과가 증폭되고 분석도 쉽지가 않다. 현재 안전관리기능이나 사고원인 발생후의 운전원의 확신적인 실수를 분석할 능력이나 또 그런 경험이 없다. 이러한 점에서 인간실수 처리에 대한 입장은 기기의 고장에 대한 지식이 현재보다 부족한 상황에서 비교적 간단한 결정론적 접근방식을 통해 기기의 무작위적 고장이 발생해도 계통이 견딜 수 있다는 확신을 얻으며 했던 원자력의 초창기와 비슷하다고 할 수 있다. 따라서 이제까지 안전관리상의 실수와 사고원인 발생 후의 운전원 실수로 체계적으로 분석하기 위한 첫 시도로 결정론적 기법을 간단하나마 소개했다. 이러한 기법이 궁극적으로는 생각할 수 있는 모든 상황을 충분히 해결할 수는 없을 것이나, 확인된 유형의 인간실수에 대처하기 위한 안전관리체계의 능력배양에 있어서는 어느 정도의 확신을 주고 있다.

기기고장에 대처하기 위한 결정론적 해석기법이 原子力發電所에서 이미 시험되어 왔으므로 아직 현재의 능력으로는 충분한 평가와 확신을 할 수 없는 인간실수분야에 비슷한 기법을 적용함이 타당할 수 있을 것이다.