한국원자력학회
'98춘계학술대회

사고관리방안의 평가를 위한 인적오류분석 기법 요건과 방향

이용희, 하재주, 정원대, 김재환
한국원자력연구소

요약

사고관리 방안의 타당성에 대한 면밀한 검토를 위하여 제안된 방안에 대한 운전원의 수행 가능성을 평가하는 과정이 있다. 수행 가능성의 평가에서 기존의 적용 사례와 인적 오류 분석 기법들을 검토하여 기존의 인간 신뢰도 분석 기법을 활용하는데 발생하는 여러가지 문제를 검토하고 새로운 기법의 요건과 방향을 제시하였다. 또한, 산업안전관리 분야에서 사용되고 있는 IAD(industrial Accident Dynamics)를 기반으로 인적오류의 가능성을 분석하는 절차를 제안하였다.

1. 서론

본 논문에서는 사고관리 방안에 대한 수행 가능성을 검토하기 위하여 보다 정성적인 분석을 제공할 수 있는 인적오류 분석(Human Error Analysis: 이하 HEA) 기법의 방향을 제시하였다. 우선, 인적요인에 대한 신뢰도 분석의 문제점을 보강하고자 기존의 기법을 검토하고, 사고관리에서 인간신뢰도 분석의 사례에 대한 민감도 분석을 통하여 문제점을 부각하고 새로운 기법의 요건을 제시하였다. 또한, 새로운 HEA 기법의 기본 체계로 산업현장의 안전관리에 사용되고 있는 IAD(industrial Accident Dynamics: 이하 IAD)를 기반으로 사고관리의 인적오류 가능성에 대한 정성적인 분석 방법을 제시하였다.

설계기준 사고를 넘는 사고 범위에 대하여 원자력발전소의 안전성 확보를 위하여 중대사고시의 대응 방안을 개발하고 있다. 사고관리에서는 가상 사고 경위를 평가하여 절차서 및 지침서 개발, 소요 정보 분석, 보조 도구와 훈련 프로그램 개발, 조직 구성 등 사고관리 체계 (Accident Management Framework) 구축하고 있다. 사고관리 방안의 평가에는 사고관리 방안의 정효과와 부작용 및 수행 가능성 등에 대한 평가가 필요하다. 제시된 방안의 수행 가능성 평가를 위해서는 운전원 행위 및 작업 내용(task), 기존 절차서와의 양립성(compatibility), 사고관리 방안 수행 관련 필요한 정보 (information needs), 필요한 정보 규정 및 제공 계측기의 역량, 관련 설비의 불이용도 (unavailability), 방안 수행에 필요한 설비 및 인원 동원 조건 등을 고려한 효과 정도 (effectiveness)에 대한 평가가 필요하다.

확률론적 안전성 평가(Probabilistic Safety Assessment : 이하 PSA)를 이용하여 사고관리 전략을 평가하면, 각 방안을 통하여 원자로의 안전성을 유지할 수 있는 가능성을 종합적으로 평가할 수 있다. PSA에서는 인간 실수와 기계 고장의 조합으로 안전성 확보에 실패할 수 있는 시나리오를 도출하고 각 시나리오의 확률을 계산한다. 그러나, 중대사고의 대응은 극도의 스트레스 상태이며 단순히 준비된 절차를 수행할 수 없을 것으로 보이므로, 운전원 혼란, 인지적 자원 분산, 부적절 상황 초래 가능성, 운전원에게 미칠 위험 등 수행 가능성을 위협하는 인적요인에 대해서는 보다 면밀한 검토가 필요하다.

2. 사고관리 방안의 인간 신뢰도 평가에 대한 검토

2.1 수행 가능성 평가의 구조

사고관리 방안의 수행 가능성은 방안의 실행과 관련된 인적 자원, 관련 기기와 정보 가용성을 포함하여, 허용된 시간 내에', '주어진 기기 및 장비를 이용하여', '성공적으로 완료' 할 가능성을 평가한다. 허용 시간이란 원자로가 노심 손상, 노심 낙하, 원자로 용기 파손, 격납건물 파손 등 중대손상 상태에 도달하기 전까지의 시간을 의미하며, 실패의 요인으로는 운전원 오류, 기기 고장, 시간 지연 등이 포함된다. 사고관리 방안의 수행 가능성을 검토하기 위한 기본 체계는 일반적인 사건 수목에서 운전원 진단 및 의사결정 오류 확률(P_{Fd}), 운전원 수행 실패 확률(P_{Fa}), 관련 기기 실패 확률(P_{Fs}), 수행시간 지연으로 인한 가용 시간 초과 확률(P_{Fr})에 대한 평가로 귀결된다. 각 사건이 독립적이라고 가정하고, 전체 수행 실패 확률(Non-Success probability: P_{NS})은 $P_{NS} = (P_{Fd} + P_{Fa}) + P_{Fs} + P_{Fr}$ 로 평가한다. 각 확률 항목에 대한 일반적인 평가의 방법이 있다. 첫째, 진단 및 의사결정 오류 확률(P_{Fd})과 운전원 수행 실패 확률(P_{Fa})은 순수한 인적오류 확률이다. 운전원 진단 및 의사결정 오류는 시간관계 곡선(Time Correlation Curve)과 운전원 진

단 가용시간으로부터 인간오류 확률 추정하며, 운전원 수행 오류 가능성도 Swain HRA-Handbook 으로부터 계산한다. 둘째, 작동 기기의 고장 확률(P_{Fs})은 고장 모드별 기기 신뢰도 자료를 활용하여 평가한다. 고장모드에는 요구시 고장(Failure on Demand)과 운전중 고장(Failure during Operation)이 있는데, 사고관리 관련 기기의 운전중 기능 상실의 확률은 거의 무시할 수 있는 수준이므로 요구시 고장을 중심으로 평가한다. 마지막으로, 가용시간 초과 확률(P_{Fr})은 각 시간 요소에 대해서는 별도로 면밀한 분석을 수행한다. 우선, 가용시간 내에 방안을 완료하지 못할 확률 P_{Fr}= Pr(총 방안수행시간 >전체 가용시간)에서, 전체 가용시간은 어떤 방안도 수행되지 않았을 때 노심노출로부터 노심낙하까지 열수력 분석 결과 시간이다. 총 방안수행시간(Tr)은 기기의 완료 시간(Ts)에 운전원의 진단시간(Td)과 수행시간(Ta)을 합한 값이다. 전체 가용시간과 운전원 반응 실소요 시간 및 기기 조치 완료 시간의 확률분포를 비교하여 시간 초과 가능성을 계산한다.

2.2 인간신뢰도 분석 사례 및 검토

사례를 통하여 기존의 인간신뢰도 분석 방법을 검토하고자 한다. 사례는 전원상실 사고시 원자로 공동 충수 방안으로 전원상실 사고시 운전원이 노심출구 온도 계측기(Core Exit Thermocouple)를 이용하여 노심노출을 감지하고, 격납건물 살수계통(CSS) 이용 용융노심 낙하전 원자로 공동에 물을 공급하여 원자로 공동을 범람 또는 충수시킴으로, 침수된 원자로 하단부를 통하여 원자로 외부로 열전달하고 원자로 파손을 방지하거나 파손 시점을 지연시키는 방안이다. 우선, 작동중 기기 고장 발생 확률은 10^{-5}~10^{-6} 이하로 거의 무시할 만한 수준이므로, CSS 주입 모드 요구시 고장/실패 확률만 고려한다. 진단 오류 확률은 진단 및 의사결정 가용시간 30 분 이상의 경우이므로, Swain HRA Handbook 에서 오류값을 얻는다. 방안의 핵심 행위인 CSAS 수동 발생의 수행 오류확률은 ASEP 의 Step-by-step, Extremely High Stress 로 부터 확률값을 얻는다. 마지막으로, 가용 시간 초과 확률(P_{Fr})이다. 우선, MAAP code 에 의한 노심의 용융 낙하 시간(Core Slumping Time)을 평균 μ 96.4 , 표준편차 σ 20.2 로 계산하고, 운전원 수행시간은 평균 10 분, 표준편차 4 분으로 계산하여 총 방안수행시간 분포(f_{Tr}) 를 도출한다. 그러므로, 총체적을 CSP 유량률로 나누어 얻는 공동범람 소요시간 보다 최종 가용시간 초과 확률을 확률분포로부터 계산하는 방식이다. 여기서 모든 시간 분포는 이변수 와이블을 사용한다. CSS 를 이용한 공동범람 방안의 종합 성공 확률(P_S)은 $P_S = 1 - P_{NS}$ 의 관계로부터 최종적으로 약 0.912 의 값을 얻을 수 있다(**참고문헌 1 참조**). 다음 표 1 은 기존의 인간신뢰도 분석에 의한 평가에 대하여 문제점을 파악하기 위하여 수행한 민감도 분석 결과를 요약한 것이다.

표 1. 성공 확률(P_S)의 민감도 분석

		P_{Fd}	P_{Fa}	P_{Fs}	P_{Fr}	P_{NS}	P_S
performance time (μ, σ) in min	Optimal case(6, 2)				2.51E-02	7.724E-02	0.923
	Base case(10, 4)				3.62E-02	8.834E-02	0.912
	Worst case(20, 10)				9.42E-02	14.62E-02	0.854
available diagnosis time in min	T=10	0.1				18.73E-02	0.812
	T=20	0.01				9.734E-02	0.910
	T=30	0.001				8.834E-02	0.912
	T=60	0.0001				8.744E-02	0.913
task/ stress	Dynamic/extremely high		0.25			28.83E-02	0.712
	Step-by-step/extremely high		0.05			8.834E-02	0.912
	Step-by-step/moderately high		0.02			5.834E-02	0.942

운전원 수행시간 분포(f_{Ta})에 따른 민감도 분석 결과, 평균 수행시간 6~20 분, 표준편차 2~10 분의 범위에서 운전원 수행시간의 변화로 인한 시간 지연에 의한 실패 확률 P_{Fr} 은 70~250 % 까지 변화하지만, 전체 성공확률 P_S 은 10 % 이내의 변화를 보이므로 수행 시간이 전체 성공 확률에 미치는 영향은 적다. 진단 오류 확률 P_{Fd} 는 전체 실패확률에서 비중이 작으며, 가용 시간에 대한 전체 성공확률의 민감도도 급격하지 않다. ASEP 으로 평가된 수행 실패 확률 P_{Fa} 는 직무 유형과 스트레스 수준에 따라 전체 성공확률에 큰 영향을 미친다. 모든 상황이 최악일 경우를 가정하면 성공확률은 0.56 까지 떨어지지만, 이러한 확률적인 계산 결과가 계측기 가용도, 사고 현상에 대한 운전원 지식 정도, 관련 절차서 유무, 훈련 정도요건, 구성 조직, 진단 및 의사결정 지원 시스템 필요성, 가용 시간 배분, 제어실 설계, 절차서의 구성 등 사고관리방안의 구성요소나 영향 요인의 선택이나 설계에 대해 유용한 정보를 제공하지 못한다. 그러므로, 인적오류를 야기할 수 있는 영향 요인의 존재 여부와 수행 실패 경로에 대한 분석이 필요하다.

인간 신뢰도 분석(HRA)은 단위 작업의 신뢰도를 확률적으로 계산하여 전체 시스템의 안전성을 평

가하는 인적 오류 평가의 방식으로, PSA 에서는 각 시나리오에서 인간에게 요구되는 직무의 수행 가능성을 확률로 계산하여, 인적오류 확률(Human Error Probability : HEP)을 제공하는 것이다. HRA 에 대한 이러한 정량적 요구로 THERP, HCR, HCR/ORE, SLIM, STAHR 등 현재 사용되는 기법의 대부분이 인적 오류의 내용보다는 오류 확률의 정량적 수준을 파악하는데 치중되어 있다. 이러한 HRA 기법들의 편중으로 인하여 평가 후에 구체적인 인적오류 감소 방안을 제시하지 못하고 있다. 그러므로, 사고관리 방안의 평가를 위해서는 수행 실패 확률을 계산하기 이전에, 작업 수행에 미치는 영향과 시스템에 미치는 결과를 중심으로 가능한 오류 및 그 요인들을 체계적으로 검토하는 HEA 과정이 보강되어야 한다.

3. 인적오류 분석의 요건과 제안 방향

3.1 인적 오류분석 기법의 요건

오류는 인간의 작업 성능에 대한 반대적인 표현에 불과하다. 오류에 대한 이해와 분석은 사람이 수행한 작업의 내용을 '오류'라고 하는 특정한 시각(view point)과 척도(measure)로 바라보는 것이다. 인적오류의 분석(HEA)은 오류의 형태 (External Error Mode), 오류의 원인 (error causes), 발생과정 (Psychological Error Mechanisms)을 밝혀내는 것이다. 오류의 분석에 사용되는 기법으로는 MORT 나 FTA 처럼 사고 분석의 일반 기법들을 연장하여 인적 오류에 대해서도 동일한 맥락으로 적용하는 경우가 많다. HRA 기법의 한계를 극복하기 위하여 현재까지 개발된 HEA 기법 중 GEMS, SHERPA, PHECA, Murphy Diagram, CADA, HRMS, COSFAH 등의 적용 범위, 오류 분석 구조, 분석 대상, 오류 분석 범위, 기반 모델 등에 대해서 검토하였다. 대부분의 기법들이 retrospective 또는 prospective 분석에 사용될 가능성이 있으나, retrospective 인 경우에는 필요한 것을 선별적으로 분석해야 한다는 점에서, prospective 인 경우에는 기법의 실제 타당성(validity)에 주의해야 한다. 사고 관리에서 효과적인 오류 분석을 위하여 필요한 요건은 다음과 같다.

(1) 오류의 종속성 : 인적 오류를 독립적인 분석 대상으로 생각하면, 오류의 형태나 오류 발생시 인간의 인지적 내부 구조에 대하여 상당히 흥미로운 연구가 가능하다. 그러나, 이러한 연구는 인지심리학의 학문적인 연구 대상으로 널리 활용되어 왔다. 그러나, 인지심리학의 연구는 오류 발생을 방지하는 것과는 일단 거리가 있다. 체계의 일부로서 사람의 행위가 어떠한 피해를 발생시켰거나 그 가능성을 가지고 있어서 이를 방지하려는 목적으로 오류를 파악하려 한다면 보다 직접적이고 실제적인 분석이 필요하다. 오류는 수행한 작업의 일부분으로 전체 체계의 기능이 작용하는 과정의 일부분으로 분석되어야 하며, 인지적 구조에 대한 독립적인 분석은 필요할 경우에 국한한다. 오류의 사건에 대한 이러한 종속성 때문에, 오류에 대한 자료도 반드시 상황과 시스템에 대한 정보와 결합되어 있을 경우에만 의미가 있다.
(2) 오류의 잠재성 : 오류를 빙산에 비유하는 것은 안전 공학의 오랜 전통이다. 오류가 발생하면 유사한 오류 또는 그 가능성이 빙산의 하부처럼 커다랗게 존재하고 있다는 것이다. 산업계의 실적 자료를 이용하여 1:29:300의 비율을 잠재적인 오류의 비율로 제시하기도 하는데, 그 비율은 해당 산업에서 다루는 시스템의 복잡성(complexity)에 비례하는 것으로 파악된다. 즉, 복잡한 시스템일수록 인적 오류가 잠재될 가능성이 크며, 알려지지 않는 오류가 많다는 것이다. 또한, 오류의 피해도 빙산에 비유된다. 직접적인 비용에 비하여 후속 조치 등의 간접 비용이나 관리비용, 사기 저하 등 파급효과를 고려하면 빙산과 같이 보이지 않는 막대한 비용이 발생한다는 것이다. 그러므로, 오류 분석에서 이러한 빙산의 드러난 표면만을 다루어서는 효과적인 오류 방지를 달성하지 못하므로, 오류가 가진 잠재성에 따라 심층 구조를 파헤치는 작업이 필요하다는 것이다.
(3) 오류의 단계성 : 오류의 비독립성에서 지적하였듯이 인간의 오류는 전체 체계의 거동에서 파악되어야 한다. 오류는 배경 요인으로부터 오류 발생을 야기하는 환경 및 체계의 불안전 상태, 불안전 행위, 불안전 행위로 인한 체계의 반응 및 손실 등이 시차를 두고 동적으로 나타나는 것이므로, 반드시 여러 단계의 구조를 가지고 파악되어야 한다. 이러한 오류의 단계성을 안전 공학에서는 도미노에 비유하였다. 일명, 도미노 이론이라고 불리는 안전 공학의 개념에 의하면, 사고의 발생은 환경 -> 인적 결함 ->불안전 행위 또는 불안전 상태 -> 사고 -> 상해 또는 피해 등의 다섯 가지 단계를 거쳐서 발생한다는 것이다(Heinlich, Bird 등). 다섯 가지 단계가 무엇인지에 대해서는 새로운 이론들이 있을 수 있으나, 도미노의 연쇄성을 보면 어느 하나라도 잘 처리되면 연쇄 작용의 고리를 끊어 사고를 방지할 수 있다는 것이다. 또한, 이러한 여러 가지 요인들의 연쇄성으로 볼 때, 전체 연쇄 구조(chain structure)의 강도는 가장 취약한 고리의 강도에 의해 결정되므로 인적 결함에 의한 불안전 행위의 야기라는 고리가 분석의 핵심으로 다루어야 함을 알 수 있다. 이러한 개념은 사고의 방지 측면에서 가장 개선 효과가 큰 접근 방식을 확보하는데 중요하다. 그러므로, 이러한 요건들은 오류의 분석은 관련되는 사건의 일부로 이

루어져야 하며, 오류의 표면적인 내용보다는 사건의 내부 구조를 형성하는 요인들과 그 잠재적인 영향을 예지하는데 주된 목적이 있음을 의미한다. 분석에서 주로 다루는 오류의 원인이나 형태에 대한 분류 체계는 오류의 단계성과 비독립성에 의하여 매우 폭넓은 구조를 가지도록 구성해야 함을 알 수 있다. 또한, 목적하는 바 오류 방지를 위해서는 원인의 분류 체계가 실행 가능한 대응 조치와 밀접한 관련을 가지고 구성되어야 한다. 오류의 방지를 위해서 더욱 중요한 것은 near-miss와 같은 값진 정보에 주의해야 하며, 오류 사례들을 주어진 인간-기계 체계의 내부 구조로부터 발생 가능한 최대한의 잠재적인 영향의 가능성을 인식하는 계기로 삼아야 한다는 것이다.

HEA 의 대표적인 기술적인 흐름으로 분류 체계(taxonomy)를 이용한 기법과 모형(model)을 이용한 기법이 있다. 이러한 유형들은 오류 분석에서 대상 작업에 대한 분해(decomposition)의 기본 구조로 도입되는 것이 무엇인지에 따른 것이다. 대상 작업에 대한 분할의 기본 구조로 분류 체계를 이용한 기법은 도입되는 분류 체계에 따라 다시 오류의 외부적인 형태(external type) 분류에 관심을 두는 기법과 원인 요소(causal factor)에 대한 기법으로 구분할 수 있다. 모형을 이용한 오류 분석은 오류가 발생한 작업의 내용이나 절차에 대한 직무 모형(task model)이나 인간 자체에 대한 작업자 모형(human model)을 분석의 기본 골격으로 도입하는 것이다. 인적 오류 분석에서 사용되는 작업자 모형에는 신체적인 한계와 특징을 담은 모형(physical model)도 있으나, 대부분 인지적인 과정에 대한 모형(cognition model)으로, 인지 모형을 이용한 기법이 다양하게 발전하고 있다. HEA에서 오류가 발생한 작업을 세부적으로 살펴보기 위하여 사건의 분해(decomposition) 과정이 공통이나 어떤 기준으로 얼마나 세분하는가에 대해서 다양하다. 우선, 오류가 발생한 사건의 맥락에서 작업자의 작업을 분리하여 별도로 분석해야 하는가의 문제가 있다. 어떤 사건을 인간과 기계의 상호작용으로 보면, 각각 인간 작업자의 행동과 기계(및 환경)의 거동으로 양분할 수 있다. 인간의 행동과 기계의 거동에는 각각 별도의 원칙과 기준이 있으므로, 많은 방법들이 어느 한편에 대하여 각각의 논리를 따라 분석하도록 하는 일반적인 방법을 취하고 있다. 인간 작업자의 행위 자체를 분석하고자 할 때, 작업의 내용에 대한 분할 방식과 기준을 다루는 것이 직무분석(task analysis) 기법이다. 인간과 기계를 양분하여 별도의 논리로 분해하거나 직무분석에서 인간 작업자의 논리만으로 분석하는 데는 위험이 있다. 어느 한편의 기준에 의하여 분해 과정을 진행하므로, 사건의 실제 상황에 대한 정보를 상당히 놓칠 수 있다. 전체 사건의 맥락을 유지하도록 분해하는 것이 중요한 요건이다. 즉, 사건에서 인간 작업자의 작업 내용과 기계의 거동이 어떠한 상호작용으로 진행되었는지를 분석 결과에서도 유지하는 것이 중요한 요건이다. 분석의 기본 체계가 실무적인 분류 체계이든지 아니면 보다 체계적인 모형이든지 보다 중요한 것은 어느 한편의 논리로 일방적으로 다루어지지 않아야 한다는 것이 HEA 기법의 요건이다. 작업자의 작업 행위만을 다루는 기법은 실제 응용 분야에서 실효성에 한계가 있다. 오류 분석의 실효성을 위해서는 사건의 전체 진행을 포괄적으로 다루면서 사건의 일부분으로 포함된 작업자의 행위와 작업 행위 속에 내재된 오류를 파악하는 것이 필요하다. 세부적인 한 부분을 다루는 기법들보다는, 보다 근원적으로 사건 전체를 다루는 안전 공학의 일반적인 기법들에 주목하였다.

IAD(Industrial Accident Dynamics)라는 사고 분석 기법을 근간으로 사고 관리에 적합한 인적 오류 분석 기법의 방향을 제시하였다. IAD 는 사고의 전체적인 맥락을 파악하는데 사용되어온 안전 공학의 일반적인 사고 분석 접근 방법의 하나이다. IAD 는 사건과 관련된 요인과 이러한 요인들의 상호작용을 표현하는 단계에 의하여 matrix 방식의 기본적인 분석 체계를 제공하고 있다. 그림과 같이, 횡축에는 사건의 발생 단계를 열거하고 종축에는 사건과 관련된 요인들을 열거하여 분석의 기본 틀로 활용한다.

	background factor	background initiating factor	initiating factor	intermediate factor	immediate factor	near accident	accident	measurable result	counter-measure
Machine									
Man									
Media									
Management									

그림 1 . IAD 의 분석 체계(worksheet 양식)

IAD 기법의 전체적인 구성은 사고의 내면 구조를 포함하는 단계 분류와, 사고와 관련된 object 를 중심으로 하는 요소들의 분류 체계를 포함하고 있다. 단계 분류는 background factor 로부터 initiating factor 를 거쳐 counter measure 에 이르는 사고의 단계를 7 단계(또는 6-8 단계)로 분류하였다. object 의 분류는 4M(Man. Machine, Media, Management)으로 분류한 다음 각 세부 요소들을 열거하였다. 각 세부 요소들이 사건의 어느 단계에 이르기 까지 영향을 미칠 수 있는 것인지에 대하여 개별적으로 파악하여 기본 자료를 확보하지만 특정한 분류 체계나 단계를 명시하는 것은 아니다. 이러한 구성은 오류의 종속성을 따라 사건 전체의 맥락에서 오류를 분석할 수 있게 할 뿐만 아니라, 단계성과 잠재성을 포착하는데도 중요하다. IAD 에서 기본적인 분석 체계를 제공하고 있기는 하지만, 사고 관리라는 특정 분야에서 활용 가능한 기법을 확보하기 위해서는 전반적인 수정 보완이 필요하다. 안전성 분석의 다른 분석 기법들에 비하여 IAD 는 다음과 같은 측면에서 상대적인 특징과 장점을 가지고 있다.

- 사건의 내부 구조를 명시하도록 유도함으로써 사건의 내용과 성격은 물론 원인에 대해서도 귀납적 연역적 해석이 가능하다.
- 원인과 사건의 진행 내용을 분리하지 않고 실제 발생의 내부 구조를 시각적으로 제시할 수 있다.
- 사건과 관련된 요인들의 변화에 대하여 What-if 방식의 민감도 분석이 가능하다.
- 간단하게 FT/ET 를 작성할 수 있으므로 정량화를 직접적으로 지원할 수 있다.

IAD 의 이러한 구조는 매우 일반적이므로 특정한 응용 분야에서 적용하기 위해서는 IAD 의 두가지 중심축에 대한 재설정이 필요하다. 다음은 IAD 의 적용을 위한 분석 절차를 간략하게 요약한 것이다.

(1) 우려되는 사건을 정의한다.
(2) 사건과 관련될 수 있는 요인들을 조사한다.
(3) 요인들의 속성과 영향을 조사하고 분류체계를 구성한다.
(4) 사건의 단계를 정의하고 background 로부터 귀납적 또는 연역적으로 요인간의 관계를 추적한다. (세부 단계 필요)
(5) 요인간의 관계를 이용하여 critical path 및 minimal cut set 을 도출한다.
(6) 사건의 발생에 관계된 요인들의 상대적인 중요도를 평가한다.
(7) 요인들의 영향을 제거할 수 있는 방지대책을 수립한다.

사고관리 방안의 평가를 위하여 IAD 를 적용하기 위해서는 다음과 같이 다섯 단계로 확장된 분석 과정을 제안하였다. 가능한 시나리오를 도출하고 영향 요인들을 파악하기 위한 과정이다.

- 오류의 형태에 대한 이해 및 조사 : 문헌, 인터뷰 등
- 가능한 오류라고 생각되는 것은 우선 열거 : 타당성 검토 없이 brainstorming 방식
- 제시된 오류 평가 : 타당성과 중요도에 대한 상대적 평가
- 제시된 오류들에 의한 가능한 사고 진행 경위 구성
- 각 시나리오의 평가 : 구체적인 가능성과 타당성 검토

표 2. 가능한 시나리오 및 사고경위별 주요 인적요소 분석

			6	7	8	15	16	17	18
1	초기 사고후 CD 도입시간		> 11 hr						~ 1 hr
2	시스템 거동 (온도, 압력 등)								
3	인적자원 및 조직	1) TSC 조직 구성 가능성	Yes						No
		2) 가능한 현장 작업							
		3) 현장 작업시 인적 자원							
		4) 현장작업시 의사소통 방법							
		5) 수작업 정도							
4	기기 구성 변화	HPSIS 가동 유무	Yes	No	No	Yes	No	No	No
		RWT-CSS Lineup 변화 가능성							
		현장작업시 밸브조작 가능성							
		기타 필수계통 상황 (전원 등)							

5	MCR 상태: Alarm 발생 Rate	Low						High
6	Multiple Strategy 또는 추가 가능성							
7	number of Failed System							2
8	절차서 Description 상세 정도							
9	기타 영향 인자							

제안된 방안을 따르면, 원자로 용기의 파손 방지를 위한 공동범람 방안을 수행하기 위하여 노심상태 진단과 수위 측정 계측기: RVLMS (Reactor Vessel Level Monitoring System) 및 노심출구 온도계측기(Core Exit Thermocouple)의 감시로부터 방안의 수행에 필요한 운전원의 작업은 정전사고시 노심 상태 및 노심 수위에 관한 정보 지속적으로 관찰 -> 전원 회복 확인 -> 적절한 시점에서 CSS 강제 기동(관련 절차서의 참조->해당 기기 제어 판넬로의 이동->제어 판넬 조작) 등으로 매우 단순하다. 보다 면밀한 분석을 위해서는 단계의 세분과 형태에 대한 재분류가 필요하다. 우선 방안의 전체적인 수행 단계를 '진단/의사결정 -> 실행' 세분하는 것은 가능하지만 보다 신중한 체계가 필요하다. 라스무센 모형과 같은 인지단계 모형의 단계를 적용하면, 진단/의사결정 이전에 감지 단계로부터 다양한 형태의 인적오류 분석이 가능하게 된다. 실행 이후의 기기 가동 완료 이전에 다양한 운전원 오류의 개입으로 방안의 수행이 저지될 수 있다. 또한, 오류의 형태에 대해서는 Swain 이 제시한 Error of Omission, Error of Commission, Extraneous Act 등 분류 체계가 있으나 이러한 외적인 오류 형태 분류만으로는 인적오류 감소를 위한 구체적인 방안을 제시하기가 어렵다. 구체적인 인적오류 감소 방안을 제시하기 위해서는 인적오류 외적인 형태 뿐만 아니라, 인적오류의 발생 원인과 과정을 밝혀내야 한다. 이러한 상세한 분석은 인간신뢰도 분석에서 보다 신뢰성있는 확률을 얻도록 반영된다.

5. 결론

본 논문에서는 다양한 가능한 오류 내용을 열거하는 방법을 중심으로 새로운 HEA 기법의 요건과 방향을 제시하였다. 방안의 수행 직무 내용을 기준으로 이미 언급된 많은 가능한 오류 형태를 기준으로, 주어진 사고 관리 방안에서 발생 가능한 보다 다양한 가능한 오류 내용을 열거하는 방안으로 IAD 를 기반으로한 기법을 제안하였다. 제안된 기법에서는 가능한 오류를 발견하고 영향관계를 구성하는 체계적인 방법이 핵심적인 내용인데, 유사한 사례로 COSFAH (Computerized Support For Analyzing Human-errors)를 비교할 수 있다. COSFAH 에서는 인적오류를 포함한 작업행위에 대하여 인지적 수행 단계를 역추적함으로써 인지적 오류의 원인을 분석하며, 작업의 내용을 역추적하는 기반으로 간략화된 인지단계 모형을 사용하고 있으며, 단계별로 오류의 형태 (type)와 원인(cause)을 연결하는 동적인 분류체계(dynamic classification scheme)를 가지고 있다. 그러나 COSFAH 는 retrospective 한 기법이라는 측면에서 상당히 다르다. 추후 연구방향으로 오류분석을 위한 인지적 직무분석(cognitive task analysis)의 중요성이 부각되고 있다. 대부분의 기법들이 오류분석을 위한 인지적 직무분석을 위하여 모형 기반 접근방식(model-based approach)을 시도하고 있으나, 실제 운전원이 경험하는 정보부담을 기준으로한 사례(1996, Lee & Yoon)에서 보다 현실적인 분석이 가능한 기법을 접목할 수 있을 것으로 기대된다.

[참고문헌]

1. 이용희, 원자력발전소 사고관리 방안의 인간 신뢰도 분석 및 오류 가능성 도출 대한인간공학회'97 추계학술대회발표논문집
2. B. Kirwan, "The Development of A Nuclear Chemical Plant Human Reliability Management Approach: HRMS and JHEDI", Reliability Engineering and System Safety, Vol. 56, pp. 107-133, 1997.
3. W.C. Yoon, Y.S. Kim and Y.H. Lee, A model-based and computer-aided approach to analysis of human errors in nuclear power plants, Rel. Eng. and System Safety, vol.51, pp.43-52, 1996.
4. Y.H. Lee and W.C. Yoon, A cognitive task analysis method for the procedure-based tasks in nuclear power plants, Proc. CSEPC'96(Cognitive System Engineering in Process Control), 1996.