'99 추계학술발표회 논문집
한국원자력학회

원전에서 전산화 도입으로 인한 인적오류 가능성 분석의 기본 체계
(A Basic Framework for the Analysis of the Human Error Potential due to the Computerization in Nuclear Power Plants)

이용희

한국원자력 연구소
대전광역시 유성구 덕진동 150번지

요약

원자력 발전소 설계에서 전산화의 도입시 예상되는 막대한 효과를 실현하기 위해서는 안전성 측면에서 전산화가 내재하고 있는 문제를 시급하게 확인해야 한다. 그중에서 인적오류의 가능성에 대한 점검이 필수적이다. 전산화가 운전기능은 물론 인터페이스에서 경험되는 운전원의 의식에 상당한 변화를 야기하는데, 그 결과로 우려할 만한 새로운 형태의 오류가 발생하지 않음을 검증해야 한다. 그러므로, 전산화의 도입으로 예상되는 긍정적인 측면과 부정적인 측면을 인적오류의 가능성과 관련하여 파악할 수 있도록 새로운 인적 오류 검토 체계가 필요하다. 본 논문에서는 원자력 분야에서 기존의 인적오류 연구 방법론을 검토하고, 전산화의 도입으로 예상되는 새로운 오류의 가능성을 파악하는 기본 체계를 제시하였다.

Abstract

Computerization and its vivid benefits expected in the nuclear power plant design cannot be realized without verifying the inherent safety problems. Human error aspect is also included in the verification issues. The verification spans from the perception of the changes in operation functions such as automation to the unfamiliar experience of operators due to the interface change. Therefore, a new framework for human error analysis might capture both the positive and the negative effect of the computerization. This paper suggest a basic framework for error identification through the review of the existing human error studies and the experience of computerizations in nuclear power plants.

1. 서론 및 배경

공정제어체계의 전산화는 기술적인 측면은 물론 경제적인 측면에서도 큰 효과를 가져오는 것으로 인식되고 있다. 인간공학적 측면에서도 전산화는 운전의 편의성 향상, 운전원 지원기능의 강화 등을 통하여 매우 긍정적인 효과를 가져온다는 것이 실증되고 있다. 원자력 발전소에서도 전산화의 도입은 필연적인 미래로 보이며, 다른 산업에서 경험 또는 예상하는 효과와 동일한 효과를 얻을 수 있을 것이다. 그러나, 원자력의 안전성 보장에 대한 요구가 평균적인 기능 및 효율의 향상보다는 최악의 경우에 대한 대비를 요구하는 보수성을 전제로하고 있어서 전산화에 대한 의사결정은 단순하지 않다. 특히, 인간공학적인 측면에서는 전산화로 인하여 운전기능의 전반적인 향상을 누구도 부인하지 않으나, 새로운 형태의 인적오류에 대한 우려가 해결되지 않은 상태이다.

본 논문은 원자력발전소의 설계에서 전산화의 도입 및 그에 따른 여러 가지 변화로 예상되는

인간공학적 문제점을 인식하는 출발점을 제공하려 한다. 인적오류에 대한 기존의 연구에 대한 검토로 전산화의 오류 가능성을 검토하는데 예상되는 한계를 검토하고, 원자력 발전소에 이미 도입된 전산기능의 경험과 전산기능에 대한 일반 산업의 경험으로부터 발생 가능한 인적오류의 범위와 그 영향 정도를 적시하는 틀을 제시하고자 한다.

2. 기존 방법에 대한 검토

인적오류(Human Error)는 인간이 주어진 일을 수행하지 못하거나 금지된 행위를 함으로써 시스템에서 요구된 기능 완수에 실패하는 것으로 정의할 수 있다. 인적오류의 발생은 때로는 심각한 결과를 초래할 수 있기 때문에 인적오류를 줄이기 위해 다양한 분석이 연구되었다. 원자력 분야에서는 전체 시스템의 신뢰도를 추정하기 위해 수행되는 확률적 위험도 평가(Probabilistic Risk Assessment : PRA)의 일환으로 수행되는 인간신뢰도 분석(HRA)이 인적오류 분석의 핵심이다. HRA 방법을 구분하면, 인적오류 분석(Human Error Analysis: HEA)의 촛점에 따라 오류의 원인(source)에 관심을 집중하는 하향식 분석과 오류발생의 결과(consequence)에 관심을 집중하는 상향식 분석으로 구분하거나, 이미 발생된 오류의 원인분석을 위한 회고적 분석(retrospective analysis)과 발생 가능한 오류에 대한 예견적 분석(predictive analysis)으로 구분하기도 한다.

본 논문에서는 PRA의 일환으로 오류 확률 도출을 중심으로 실무적으로 개발되고 이미 활용된 기법을 제 1 세대 기법, 제 1 세대 기법의 한계점을 해결하기 위하여 제안된 기법들을 제 2세대 기법으로 보고 전산화의 도입에 따른 발생 가능한 인적오류의 파악 및 인터페이스의 영향 분석이라는 측면에서 그 특성을 검토하였다.

2.1 제 1 세대 방법의 검토

인적오류 분석에 대한 연구가 오래전부터 있었지만 HRA는 주로 1970년대부터 본격적으로 시작되었다. HRA 방법의 개발 연도를 보면 1970년대 후반에 시작되어 대부분은 1980년대 초반에 개발되었고 1980년대 후반으로 가면서 개발된 방법의 수는 점차 줄어들었다. 물론, 1990년대에도 몇가지 새로운 방법들이 제안되기도 하였지만, 그 수는 1980년대 초에 비해 현저히 적었다. 이는 1979년 발생되었던 TMI사고의 발생과 무관하지 않을 것이다. 즉, 많은 사람들이 TMI 사고로 원전에서 인적오류분석의 중요성을 공감하였고, 그에 따라 새로운 HRA 방법의 개발을 노력하였기 때문이다. 현재 인적오류분석에 활용할 수 있는 방법들은 대략 35-40가지 정도나 된다. 그러나, 몇몇은 1960년대에 최초로 제안된 THERP(Technique for Human Error Rate Prediction) 등의 변형에 지나지 않고, 명확하게 구별할 수 있는 것은 그렇게 많지 않는 것으로 파악된다.

따라서, 기존의 HRA 분석 방법들에 대한 기술적 수준에서의 비교를 다음 표와 같이 요약하였다. 원자력발전소에 전산화가 도입될 경우 작업특성이 여러 가지 측면에서 변화될 것이기 때문에 각 방법의 적용방법, 분류체계, 운전원 모델, PSF의 영향 고려 등에 대하여 살펴보았다. 이러한 방법들에 대한 비교 분석의 예를 들면, Dougherty & Fragola (1988)는 시스템 공학적 접근 방법을 설명하였는데, 주로 THERP에 초점을 맞추었다. 또한, Park(1987)는 인적오류와 그것의 방지에 더 많은 초점을 맞추었는데, 주된 관심은 THERP, OAT(Operator Action Tree), 그리고 여러 가지의 결함수(fault-tree)방법의 활용에 대한 설명을 포함하고 있다.

OAT, THERP, SLIM/MAUD, HCR 등 적용절차가 상세하지만, 가장 중요한 오류분류체계가 상세하지 못하거나 항목들에 대한 정의가 불확실하고 오류모드를 고려하지 못했다. 따라서, 정량적인 확률 도출 측면에서는 명확하지만 실제로는 전산화에 따른 발생 가능한 오류의 가능성을 평가하거나 인터페이스의 변화의 평가 목적에 따라 상당히 다르게 적용될 수 있다. 그리고, 대부분의 방법에서 운전원의 내부 과정 모델을 고려하지 않고, PSFs에 대한 고려도 매우 제한적이다.

HRA 방법	방법설명	분류체계	운전원 모델	PSF 영향	확장 가능성
AIPA	상세하지 않음	성공/실패	블랙박스(TRC)	고려안됨	불확실
Confusion matrix	기본적 원칙 설명	부적절한 진단	없음	고려안됨	인지분야 가능
OAT	상세한 절차 제공	부적절한 진단 (성공, 실패)	단순한 단계모델 이지만 TRC에 중점	고려안됨	직무분석 가능
STAHR	기본적 원칙 설명	없음	없음	영향도에 의해 적용	PSF분야 가능
THERP	상세한 절차 제공	작위 부작위 시간초과	S-O-R 시간초과는 SRK 인용	정량적으로만 고려	(기초기법)
전문가 추정	기본적 원칙 설명	명백히 정의되지 않음	없음(잠재적)	함축적 및 정량적으로만 고려	불확실
SLIM/MAUD	상세한 절차 제공	명백히 정의되지 않음	없음	정량적으로만 고려	PSF분야 가능
HCR	상세한 절차 제공	성공, 실패, 무반응	TRC 곡선의 선택에 대해서만 SRK 인용	정량적으로만 고려	PSF 제한
MAPPS	명백하지 않고 시뮬레이션에 포함	명백히 정의되지 않음	명백하게 정의 되지 않음	명확히 설명안됨	직무분석 가능

표 1. 제 1세대 방법의 검토 요약

STAHR(Socio-Technical Assessment of Human Reliability; STAHR)는 몇가지 상세히 검토해 볼 필요가 있다. STAHR 방법은 다음과 같은 단계로 상대적으로 꽤 복잡하다.

- 모든 적절한 조건부 사건들을 표시.
- 목표 사건을 정의.
- 중간 수준의 사건들을 선택하고 그것에 기여하는 하위수준의 영향요인 가중치 평가
- 하위수준의 영향요인에 관한 중간수준의 조건부 가중치 평가.
- 남은 중간 및 하위수준 영향요인에 대해 위의 과정을 반복한다.
- 중간수준 영향요인에 관한 목표 사건의 조건부확률을 평가한다.
- 목표 사건의 비조건 확률과 중간수준의 영향요인에 대한 명확한 비조건 가중치 계산.
- 계산결과들을 평가자의 주관적 판단과 비교 및 필요시 수정

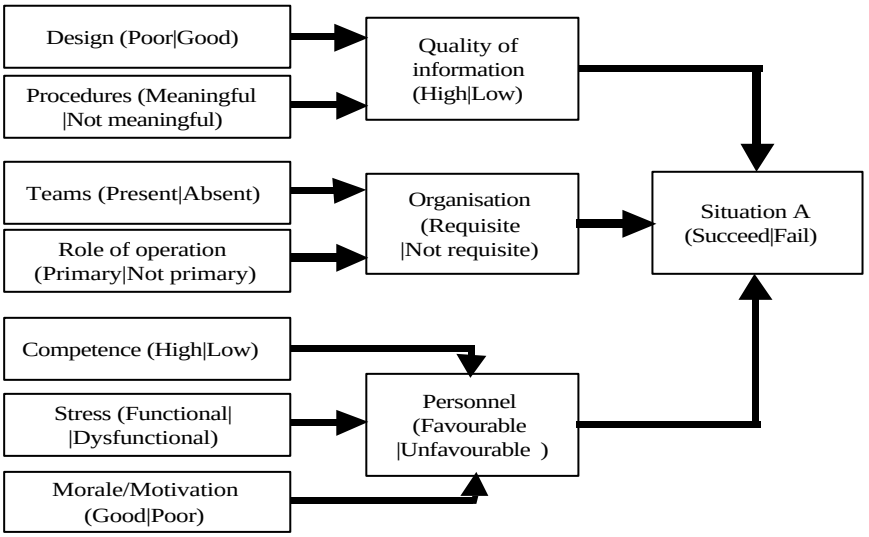

그림 1 수행영향요소의 고려 가능 방안 : STAHR 경우

- 평가자가 그들의 판단을 끝낼 때까지 위의 단계를 반복.
- 민감도분석: 점 추정치(point estimate) 또는 구간 추정치(range estimate) 기록.

이 방법은 복잡한 기술적 시스템에서 인간신뢰도를 평가하기 위한 심리적 척도 방법이고, 기술적 및 사회적 구성요소로 구성된다. 기술적 구성요소는 요인들을 상황의 결과에 연결하는 원인 및 효과의 네트웍을 나타내는 영향도이다. 사회적 구성요소는 영향도에서 나타내어진 여러 가지 요인들의 가중치와 조건부 확률에 대한 전문가 판단을 나타낸다.

STAHR는 PSA 사상수에 크게 의존하지 않기 때문에, 인간의 오류행위에 대한 고려는 미약하고 인간의 오류 행위에 대한 명확한 처리방법을 제공하지는 않는다. 그러나, 이 방법이 분해원칙에 근거하지 않기 때문에, 분리된 척도로서 PSFs를 고려할 필요는 없다. 따라서, 명확한 분류체계가 없고 인간의 오류행위에 대한 명확한 운전원 모델을 사용하지 않고, 결과에 영향을 줄 수 있는 여러 요인들 사이의 관계를 나타내는 영향도 중심의 분석 모델이다. 그러한 장점이 오히려 전산화에 따른 문제점의 분석에 가능성을 열어준다고 본다.

SLIM/MAUD방법에서는 어떤 작업의 성공가능성은 환경, 현재의 연습이나 기술의 상태, 그리고 시간 제한과 같은 PSFs 집단의 결합된 영향에 의존한다고 가정하고 있다. 따라서, PSFs의 영향을 이용하여 오류확률을 추정하고 있다. Gertman등(1992)은 PSFs의 개념을 사용함으로써 의사결정 오류에 관한 확률들을 추정하기 위한 방법을 제안했다. Zimolong(1992)은 SLIM, THERP, Raking Method들을 실험적으로 평가하기 위하여 몇개의 PSFs 집단을 사용하였다. 하지만, 이들 방법에서도 대부분 PSFs의 고려가 체계적이지 못하고, 가령 체계적이라 하더라도 다양한 PSFs가 운전원의 행위에 어떠한 영향을 미치는가를 반영하지 못하고 간편한 정량화 방안만 제시되었다.

2.2 제 2세대 방법의 검토

1세대 분석기법들 중 몇가지는 전산화에 따른 변화를 다룰 수 있는 가능성이 있으나, 대부분은 가시적인 단위 행동에 대한 실적 자료를 종합하는 정량화에 집중되어 인적오류의 가능성과 그 영향을 분석하는데는 충분하지 않다. 이는 인지적 측면에 대한 고려 결여와 분류체계의 비논리성에서 시작된다. 우선 PSA 사상수(event tree)에서 사용된 이진 표현의 개념에 따라 오류 확률평가에 집중한 결과 주어진 조작행위를 세분하여 각 단계의 성공과 실패를 분류하는 것이 대부분 방법들의 근본적 분류체계이다. 따라서, 2세대 HRA 방법에서는 두가지 기본적 요건이 보강되었는데, 개선된 PSA 사상수를 사용한다는 것과 확장된 오류모드를 포함한다.

2세대 HRA 방법들은 작업수행과정의 어느 단계에서 인적오류가 발생했으며, 발생과정이 어떠했는지를 분석하는 일반적인 분석방법과 작업자의 인지과정 모형을 고려한 분석방법으로 나눌 수 있다. PHECA(Potential Human Error Cause Analysis), Human HAZOP(Hazard and Operability) 등의 분석방법이 전자에 해당되고, GEMS(Generic Error Modeling System), Rasmussen의 연쇄적 오류분석 모형(Sequential Error Model), CREAM(Cognitive Reliability and Error Analysis Model) 등이 후자의 분석방법에 해당된다. 2세대 HRA 방법에서는 인적오류의 발생확률을 추정하는 것을 주목적으로 하는 1세대 HRA 방법과는 달리, 발생 가능한 인적오류를 찾고, 분류하고, 인적오류의 발생구조를 밝히고, 인적오류의 발생원인을 찾음으로써 최종적으로 인적오류의 저감을 위한 대응방안을 수립할 수 있는 정성적인 측면을 강조하므로 전산화의 영향을 분석하는데 보다 적합하다. 이들 모두는 전산화에 따른 인터페이스 변화 등 보다 확장된 수행영향요소의 분석에 활용할 수 있는 절차를 포함하고 있으나, 이 부분에서는 1세대에 비하여 그리 구체화되지 않았다.

2.3 기존 방법론의 보완 방향

기존의 방법론을 검토하면 현재 실제로 수행되는 인간신뢰도 분석은 주로 운전조치의 세분을 통하여 전체 실패 확률을 도출하는 과정으로 구성되어 있다. 기존의 인간신뢰도 분석은 인적오류의 가능성을 확률로 추정하는 과정에서 일반적으로 그림 1과 같은 과정을 거친다.

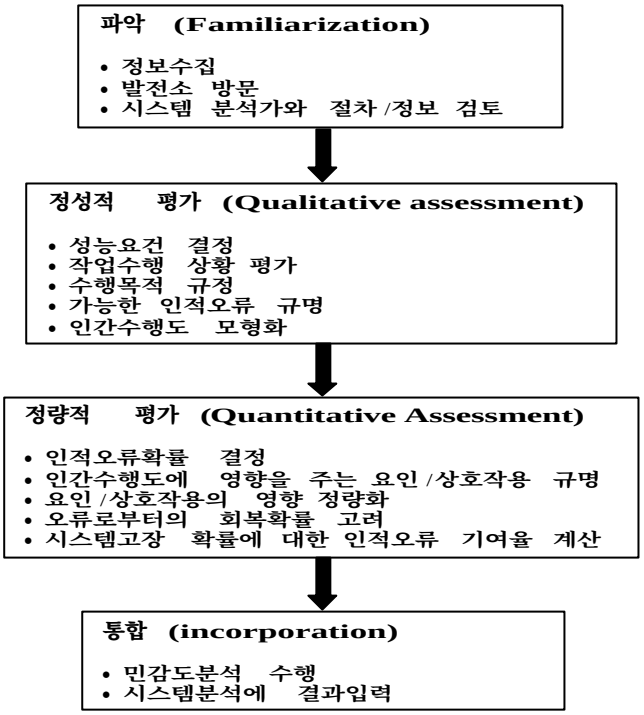

그림 2. 기존의 인적오류분석 절차

기존의 방법들을 살펴보면, 기존의 분석은 (1) 발생 가능한 모든 오류를 파악하고, (2) 확률값으로 정량화 가능하며, (3) 전체 시스템의 신뢰도 모형에 결합 가능해야 한다는 요건을 따르고 있다. 그러나, 전산화의 도입은 운전작업과 인터페이스 등의 변화가 필연적으로 수반된다. 운전원의 작업이 비가시적 또는 인지적 작업 중심으로 변화하며, 제어조작 보다는 감시 및 진단 의사결정 중심으로 전환되는 계기가 된다. 전산화의 도입에 대한 영향을 분석하는데는 기존의 방법론에서 다음과 같은 문제점을 예상되고 있다.

- 인간 수행도 모형에서 비가시적(인지적) 작업의 세분화 곤란
- 비가시적(인지적) 작업의 확률 부여 곤란
- 작업수행 영향요소(PSFs: Performance Shaping Factors)의 변화
- 새로운 조작 오류(EOC: Error of Commission)의 가능성 도입
- 작업 이전의 상황인식(SA: Situation Awareness)의 영향 급증

대부분이 HRA 기법의 모체로 THERP를 제시하고 있다. THERP에서는 작업의 스트레스 정도에 따른 몇가지의 수정인자(modifying factors)를 통하여 PSFs의 영향을 고려하고 있으나, 작업상황에 따른 인적오류확률의 수정 방법을 체계적으로 제공하지는 못하였다. 그것은 매우 낮은 작업부하(very low task load), 최적 작업부하(optimum task load), 과중한 작업부하(heavy task load), 그리고 위협적 스트레스(threat stress) 등 스트레스 수준을 네가지로 구분하여 PSFs의 영향을 고려하는 방법이다. 그러나, 고려된 내용은 단지 몇개의 수정인자(modifying factor)만을 제시하고 있고, 대부분의 PSFs는 고려에서 제외되어 있다는 것을 알 수 있다.

따라서, HRA에서 PSFs의 영향을 체계적으로 반영할 수 있는 방법의 개발이 필요하고, 또한 이들 요인들이 운전원의 작업수행에 어떠한 영향을 주는지에 대한 분석방법의 개발이 필요하다.

3. 전산화 영향 파악을 위한 인적오류 분석의 요건

우리나라에서도 이미 도입된 원전 설계를 한 차원 끌어올리는 새로운 설계 개발을 위해 노력하고 있다. 설계개선의 핵심 중 하나는 MMIS (Man-Machine Interface System)라는 명칭하에 제어실과 계측제어 기기의 개선이지만, 이는 전산기술에 근거하고 있다. 그 개선 결과가 전체 원전의 신뢰성과 효율성에 어느 정도의 효과를 가져오는지에 대해서는 인간-기계 체계 개념을 도입하여 불확실성을 제거할 필요가 있다. 또한, 새로운 설계의 도입으로 발생가능한 문제점에 대한 우려도 체계적으로 검토되어야할 필요가 있다.

다음 표2 에서 제시된 중요한 운전원 오류 가능성의 후보들은 주로 요구된 운전 조치에 대한 실패인 'fail to do somthing' 유형으로 기존의 PRA에서 THERP를 적용하여 선정되었다.

표 2. 주요 운전원 오류 항목 (초안)

#	Important Human Error Description
1	Operator fails to initiate Hot Leg Injection
2	Operator fails to perform aggressive secondary cooldown (for SGTR and Small LOCA)
3	Operator fails to maintain secondary heat removal operation (including align alternate water source)
4	Operator fails to align CVCS to fill IRWST following SGTR
5	Operator fails to perform Feed & Bleed operation
6	Operator fails to reclose ADVs on the ruptured SG-2
7	Operator fails to line up and start MFW Startup FW pump P07
8	Operator miscalibration error of bistables for SIAS
9	Operator fails to do RCS Cooldown and Depressurization (in Transient Scenario)
10	Operator fails to perform shutdown cooling operation (Injection and Long Term Cooling)
11	Operator fails to initiate emergency boration using charging pump within 1 hour
12	Operator fails to establish RCS pressure control
13	Operator fails to actuate SIAS component manually

그러나 전산화된 원전에서는 운전원의 조치 실패의 가능성이 줄어드는 반면에 오히려 인지적인 오류의 가능성이 늘어나며, 인터페이스에서 일어나는 조치들의 특성이 공간적 또는 물리적으로 분리되어 있지 않으므로 새로운 수행오류(Error of Commission : EOC)의 가능성이 고려되어야 한다. 이러한 전산화된 원전의 평가에 필요한 새로운 요건을 요약하면 다음과 같다.

- 직무의 의존성 (dependancy)의 고려
- 수행오류의 가능성 (possible EOCs)
- 인지적 오류의 영향 (cognitive factors)
- 확장된 PSFs의 고려

그중에서 인터페이스의 변경과 운전 제어 환경의 변화에 따른 확장된 PSFs의 고려 방법론이 시급하다. 차세대 원전 설계의 경우를 보면, 제어실의 기본 환경이 개인적인 워크스테이션 단위로 바뀌며 몇가지 기기가 추가 도입되었다. 우선, 물리적으로 배열된 계기 및 표시기에서 통합된 표시장치인 CRT를 통하여 수동적인 정보표시를 제공한다는 것은 매우 심각한 변화로 추정된다. 둘째, 제어기도 개별 독립된 제어기가 공간적으로 배열되어 있던 상황에서 터치 스크린을 통한 공통 제어 인터페이스를 사용하므로 제어 조작에 대한 인식의 근거가 전혀 다른 상황이 된다. 셋째, 대형정보화면과 운전원 콘솔을 기반으로 의사소통하는 방식을 취하며 좌식 작업공간으로 변화된다. 넷째, 운전절차의 전산화로 CRT를 기반으로 유사한 인터페이스를 가진 표시 및 제어 조작 기기를 함께 다루어야 한다. 마지막으로, 몇가지 지원기능을 추가하여 운전원을 돕도록 하고 있다.

전산화된 원전에서 이러한 변화 동향으로 보아 현재 인적오류 분석에서 고려되어야할 몇가지는 신뢰도 개선 측면에서 반영되지만 몇가지는 내포된 새로운 우려점을 반영하여야 한다. 현재 고려되어야할 사항은 다음과 같이 추정된다.

- 정보 및 정보 표시의 다양화
- 신체적 이동 요구 격감
- 상황 파악(situation awareness) 유지 곤란
- 진단 의사결정의 오류 가능성
- 정보 입수를 위한 정보순항의 부담
- 정보 표시의 피동성
- 오류 조치에 대한 회복 방식의 변경, 등

4. 결론 및 추후 연구 방향

전산화된 원전의 특성으로 보아 직무분석에서 오류직무에 대한 확장을 통하여 EOC와 PSFs의 고려가 새로운 분석에서 중요한 것으로 판단된다. 인간의 행위는 일반적으로 육체적, 심리적, 생리적, 환경적 요인 등 다양한 요인에 의하여 영향을 받는데, 이들을 PSFs에 대한 분석을 제공하는 체계가 시급하다. 우선, 전산화에 따른 인터페이스의 변화와 파급되는 조직 운영의 영향 등 확장된 범위의 PSFs를 고려하는 것이 필수적이다. 과거, HRA에서는 주어진 오류 확률에 대한 보완적인 차원에서 몇가지를 고려하던 것에 비하여, 새로운 체계에서는 실제로 변화되는 요인들의 오류 영향에 대하여 정/부적인 효과를 반영하는 논리가 필요한 것이다. 기존의 기법에서는 SLIM/MAUD나 STAHR에서 그 확장 가능성이 발견된다. 그러나 특정작업수행에서 PSFs의 영향을 평가하기 위해서는 AHP (Analytic Hierarchy Process)와 같은 방법이 도입될 때 보다 효과적일 것으로 판단된다. 또한, 정성적인 PSFs 요소들의 평가에 내포된 모호함을 해결하기 위해서는 정광태 등(1996)의 연구와 유사하게 퍼지이론의 반영이 요구된다.

오류의 가능성은 정량화 이전에 제공되는 오류 직무의 내용과 범위에서 골격이 결정된다. 기존의 분석에 요구되는 역할의 개별적인 실패 가능성을 확률로 표현하는데 비하여, 전산화된 원전과 같은 경우에는 직무의 범위와 무관한 새로운 조치 행위가 결과적으로 전체 기능의 실패를 야기하는 가능성이 부각된다. 이는 저출력 및 정지 운전사고 사례에서 빈번하게 목격된 불필요한 조치들의 수행오류(EOC)의 사례로 보아 분명한 현상이다. 또한, 직무간의 분할구분이 곤란할 뿐만 아니라 직무의 인지적인 특성이 부각된다. 미리 정의된 조치의 수행 실패라는 기존 분석의 한계를 넘어서는 기법은 EOC의 가능성에 대한 폭넓은 조사가 제공되어야한다. 이를 위해서는 ATHEANA (1997)와 같이 기존의 사건분석 결과에서 도출된 다양한 오류 가능성을 포함하되 보다 체계적인 오류 가능성의 범위를 검토하는 분류 체계가 필요하다. GEMS, SEM 등의 확장 가능성도 활용할 수 있다. 인지적 오류의 가능성에 대한 예견적 분석은 매우 제한적이다. 그러나, CREAM에서는 인지공학적 배경에 부합되는 오류의 기제를 제공하고 가능성을 탐색할 수 있는 체계를 보여주고 있다. 그러므로, 전산화의 영향을 파악하는 새로운 분석 체계를 시급히 개발해야 할 것이다.

참고문헌

1. 이용희 외, 차세대 원자로 인간신뢰도분석을 위한 기술현황분석, KAERI/AR-미정/99, 1999.
2. 정광태, 김인석, 차세대 원자로 인간신뢰도 분석을 위한 기술현황 자문 보고서, 1999.
3. 정원대 외, 인간오류분석 방법 비교 및 사고관리 사례 연구, KAERI/TR-998/98, 1998.