

원자력발전소 주제어실 인터페이스 설계를 위한 인적오류 분석 기법의 보완*

A Modification of Human Error Analysis Technique for Designing Man-Machine Interface in Nuclear Power Plants

이용희**, 장통일***, 임현교***

ABSTRACT

This study describes a modification of the technique for human error analysis in nuclear power plants(NPPs) which adopts advanced Man-Machine Interface (MMI) features based on computerized working environment, such as LCDs, Flat Panels, Large Wall Board, and computerized procedures. Firstly, the state of the art on human error analysis methods and efforts were briefly reviewed. Human error analysis method applied to NPP design has been THERP and ASEP mainly utilizing Swain's HRA handbook, which has not been facilitated enough to put the varied characteristics of MMI into HRA process. The basic concepts on human errors and the system safety approach were revisited, and adopted the process of FMEA with the new definition of *Error Segment(ES)*. A modified human error analysis process was suggested. Then, the suggested method was applied to the failure of manual pump actuation through LCD touch screen in loss of feed water event in order to verify the applicability of the proposed method in practices. The example showed that the method become more facilitated to consider the concerns of the introduction of advanced MMI devices, and to integrate human error analysis process not only into HRA/PRA but also into the MMI and interface design. Finally, the possible extensions and further efforts required to obtain the applicability of the suggested method were discussed.

Keyword: human error, man-machine interface(MMI), human reliability analysis(HRA), control room, failure mode and effect analysis(FMEA), nuclear power plant(NPP).

* 본 논문은 과기부 원자력 중장기 과제의 일환으로 수행되었음.

** 한국원자력연구소 계측제어·인간공학 연구부
주 소 : 302-353 대전시 유성구 유성 사서함 105호
전 화 : 042-868-2941
E-mail: yhlee@kaeri.re.kr

*** 충북대학교 안전공학과

1. 서 론

1.1 인적오류분석 기법의 필요성

안전을 최우선으로 하고 있는 원자력발전소(이하, 원전)에서는 기계적인 신뢰도 확보와 함께 인적오류에 대해 대비하고 있다. 인간신뢰도분석(Human Reliability Analysis : HRA)과 인간공학적 확인 및 검증(Verification & Validation : V&V)은 원전의 설계 과정에서 인적오류 가능성에 대비하는 핵심 과정이다(CEC, 1998). HRA는 전체 원전에 대한 확률론적 안전성 평가(Probabilistic Safety Assessment)의 일부분으로, 원전의 안전성에 끼치는 영향이 큰 인적오류 항목을 도출함으로써, 설계에서 대응방안(countermeasure)을 모색하는 출발점이다. 인터페이스(Man-Machine Interface : MMI) 등 최종적으로 설계 결과에 대한 확인 및 검증을 통해 신뢰할 만한 수준으로 인적오류가 방지되었음을 확인한다(Hollnagel, 1997). 이제까지 원전설계에 적용된 HRA기법으로는 THERP, SLIM/MAUD, HCR/TCR, ASEP 등의 1세대 기법들과 ATHEANA, CREAM, CES 등 2세대 기법들이 있다(이용희 외, 2000). 그러나, 기존의 기법들은 다음과 같은 측면에서 그 문제점과 한계를 보이고 있기 때문에 새로운 인적오류 분석 기법의 개발이 불가피하다.

첫째, 기법이 낙후되어 평가의 민감도가 떨어진다. 최신 원전에서는 주제어실 설계가 매우 급격하게 변화하고, MMI 기기나 운전방

식이 기존 주제어실과 매우 다르다. 그러나, 기존의 HRA 기법들은 인적요소를 다루는 수단이 미리 정해진 범위의 수행도 영향 요소(Performance Shaping Factors: PSFs)에 의존한다(김재환 등, 2001). PSFs 항목이 설계의 변화나 동적인 상황과 무관하게 고정적이므로, 각 항목의 값을 설계의사결정을 반영할 만큼 다양하게 변경하기 곤란하다. 따라서, 기존 기법으로는 인적요소의 급격한 변화를 HRA 평가에 반영하는데 제한적이다.

둘째, 인적오류 평가가 설계과정과 잘 연결되지 않고 있다. 현재 인적오류 평가의 핵심 과정으로 수행되고 있는 HRA는 전체 원전의 확률적 위험도에 대한 정량적 평가를 지원하는데 집중되고 있다. 활용되는 기초자료는 물론, 평가 항목 자체도 설계와의 관계가 밀접하지 않다. 따라서, 위험성 평가 결과가 설계 과정에 피드백되지 않으며, 정작 설계에서 필요한 인적요소의 평가는 개별적인 실험이나 사례 정보, 혹은 별도의 분석과정에 의존하고 있다. HRA가 세부평가나 설계의 의사결정 과정을 지원하기 어렵기 때문에, 분석 결과가 종합적인 차원에서 확인 및 검증 등 설계 실무 과정과 원활하게 연계되지 않고 있다.

셋째, HRA에서 신뢰도 평가에 포함되어야 할 오류의 범위가 확대되어야 한다. 원전의 인적오류가 실제로는 거의 경험되기 어려운 희귀사건(rare event)이라고 하더라도 아차사고(near miss)가 시스템의 상태에 따라서 그 결과가 매우 심각할 수 있기 때문이다. 운전경험상으로 발생빈도가 매우 낮은 인적오류 항목들이라고 하더라도 보다 보수적인 검출과 평가가 필요하다(Lee, 2002). 기존의 인적

오류확률 기초자료 항목들로는 전산화 및 최근에 개발된 다양한 기기와의 상호작용(interaction)에 대한 보수적인 평가가 불가능하다. 특히, 최근 운전경험검토에서 확인되고 있는 수행오류(Error Of Commission : EOC) 등에 대한 추가적인 고려 방안이 필요하다(Lee, 2002).

1.2 기술 현황 검토

인적오류분석과 관련된 최근의 연구들을 검토하면 인지모형(cognitive model) 등 운전원 모형을 도입하여 강화된 기법을 개발하거나, 실험적으로 인적오류에 대한 기초연구를 보강하는 노력으로 대별된다. 이들의 기술적인 특성을 본 연구 목적에 비추어 검토하면 다음과 같이 정리할 수 있다.

첫째, 운전원의 행위의 이면에 존재하는 내부 인지과정에 대한 관심으로 인하여 인적오류 분석에 인지모형이나 개인의 오류성향 유형 등 새로운 모형을 도입하고 있다. 이는 인적오류의 근본적인 연구를 위해서 매우 유익한 노력이지만, 안전성 향상을 위한 실질적인 방법론과는 거리가 있다. 또한, CREAM, CES, SACOM(Cheon et. al., 1997), COSIMO 등에서 보는 바와 같이 도입된 모형이 가진 가정이 근본적인 한계로 작용하므로, 분석과정의 복잡성 부담은 물론 모형에 동의하지 않는 경우에는 어렵게 얻은 결과라도 검증이 곤란하여 현실적인 반영이 어렵다.

둘째, 많은 연구들이 인적오류에 대한 실험적인 관측에 집중되어 있다. 예를 들면, 작업 상황에서 운전원의 반응특성에 따른 인지적

유형(types of task behavior) 분류(서상문 등, 1995), 개인의 오류 성향(constitution) 추적, 직무 반응시간(response time)으로부터 작업부하 추정(정원대 등, 2002) 등의 노력을 들 수 있다. 이는 매우 진지한 노력으로 반드시 필요한 연구들이지만 나름의 한계가 있다. 우선, 원전의 인적오류가 희귀사건이기 때문에 실험이나 일상적인 관측이 어렵다. 또한, 실험적 연구의 대부분 시뮬레이터를 활용하고 있어서, 운전원이 느끼는 비정상적인 부담을 모사해야 하는 실험의 사실성(fidelity) 문제를 근본적으로 해결하기 어렵다.

셋째, 인적오류와 관련된 다른 평가 척도(measures)들을 통하여 간접적으로 오류분석에 접근하는 방법이다. SAGAT, SACRI(이동하, 이현철, 2000) 등 작업부하 척도나 심전도 및 뇌파 등과 같은 생체 신호를 통하여 객관적인 자료를 확보하려는 것으로, 수치 자료에 의한 평가결과의 타당성 확보 측면에서 장점이 있다. 그러나, 작업부하나 생체신호가 인적오류와 어떤 상관관계를 갖는지에 대한 검증이 선행되지 않으면, 현실적인 결론을 얻기는 매우 어렵다. 반응시간이 지연되거나 작업부하가 높다고 오류 가능성이 높다는 것은 아직 불확실하다. 특히, 빈도가 매우 낮은 원전의 인적오류 사례나 전산화된 MMI 기기에 대한 운전원 반응을 살펴보면, 작업부하나 생체신호가 갖는 연속적인 특성과는 달리, 인적오류 가능성은 상대적으로 이산적이라고 보이기 때문이다(이용희, 1999).

넷째, K-HPES (Human Performance Enhancement System) 등 관리적인 인적오류 분석에서는 사례 중심적인 접근 방식을 취

하고 있다(Yoon & Lee, 1996). 즉, 기존에 발생하였던 사례를 중심으로 중요한 오류와 설계에서 대비되어야 할 대응방안을 도출하는 방식이다. 해당 사례에 대해서는 현실적이고 직접적인 분석결과를 얻을 수는 있지만, 사후분석이므로 hindsight effect에서 자유롭지 못하며, 많은 노력에 비해 해당 사례에만 국한된 제한적인 정보만을 얻을 수 있다.

최근에 제시된 인적오류 분석 기법이나 다양한 노력은 각기 나름대로의 장점이 있으며, 인지심리학적 기초연구나 관리적 방안으로는 반드시 필요한 것들이다. 하지만, 인터페이스 설계에 따른 안전성 평가 목적에는 불충분하거나 부분적인 것으로 파악된다. 따라서, 기술현황에서 보이는 여러 가지 기법들의 장점에도 불구하고, 원전 주제어실 인터페이스 설계의 변화에 따라 실무적으로 적용 가능한 새로운 인적오류 분석 기법 개발에 착수하였다. 본 연구에서는 기술현황과는 구별되는 고유한 관점에서 기존의 인적오류 분석 방법을 보완한 새로운 기법을 제시하고자 하였다.

2. 인적오류분석 기법의 개선

2.1 접근 방법

2.1.1 기본개념

인적오류분석에서는 개인적인 원인에 의한 오류, 기기 결함 및 파급 오류, 계통 및 기기 파급 오류, Slip 등 조작 행위 오류, 의사결정 등 인지적 오류, 의사소통 및 조직 오류, 문화 및 배경적 원인의 오류 등이 포함되어야

한다(장통일 등, 2002). 그러나, 본 연구에서는 MMI 설계를 지원하도록 분석되어야 하므로 주제어실 기기관련 오류 가능성 평가에 집중된 분석체계를 제시하였다.

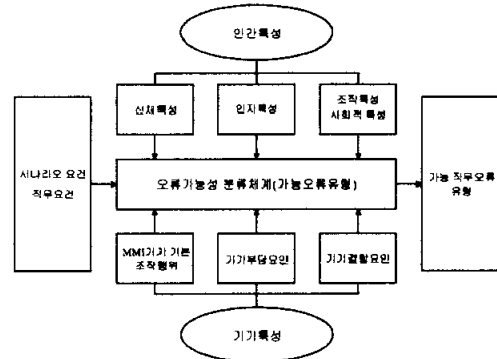


그림 1. 주제어실 MMI 기기와 관련된 오류 가능성 평가

주제어실 기기 관련 오류 가능성 평가란 그림 1에서 보는 바와 같이, 제어실에 도입된 기기의 오류 및 기기의 특성과 한계에 의하여 사용자인 운전원, 또는 기기 자체에 파급된 결함 및 오류로 파급될 가능성을 가진 항목들을 파악하는 과정이다. 전산화로 인하여 여러 가지 기능이 하나의 인터페이스에 집약된 최신 MMI 기기의 기능적인 특성과 새로 도입된 기기와 관련된 새로운 환경요소들이 운전원의 인지 및 신체 특성 요소들과 양립되지 못할 경우, 그 중요성과 크기와 무관하게 운전원의 오류를 유발시킬 수 있다는 개념이다.

기기의 안전성 측면에서는 아무런 결함이 없는 기기라고 하더라도, 기기 자체의 특성이나 한계에 의하여 설계시 전혀 예상치 못했던 행위를 운전원들이 수행할 수 있다. 운전원 자신들도 의도한 것은 아니지만, MMI 기기

의 특성에서 기인된 불필요하거나 부적절한 조작행위가 상대적으로 자주 관측된다. 이러한 의도되지 않은 행위가 시스템의 한계를 넘지 않는 범위에서 발생하면, 운전원들은 시행착오(try and error) 과정을 반복하면서 대처능력을 갖추게 되는 긍정적인 효과도 있다.

하지만, 이러한 행위의 결과가 시스템의 한계범위(tolerance) 내에서만 발생하지는 않으며, 일부는 설계시에 고려된 직무기능과는 전혀 다른 결과를 야기하여, 시스템에 부정적인 영향을 미치는 오류로 발전할 수 있다.

경로의 조합을 추적하되 최종적인 시스템에서의 영향을 기준으로 판단하도록 분석과정을 확장하였다.

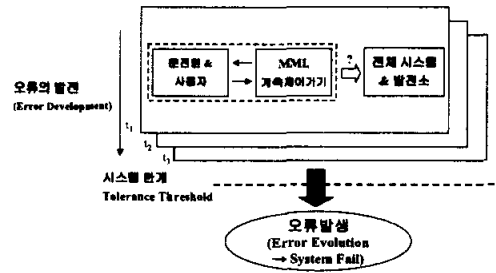


그림 2. 인적오류의 발생 개념

2.1.2 시스템 안전 기반 접근

일반적으로 인적오류라고 하면, 인간의 내부 혹은 외부의 불안전 요소가 원인이 되어 발생한 인간 자체의 문제를 가리키는 경우가 많다. 그러나, 본 기법에서 정의하는 인적오류는 이러한 개념과는 차이가 있다. 인간을 시스템의 하나의 구성요소로 보아, 시스템 전체에 결과적으로 바람직하지 못한 영향을 미치거나 그럴 가능성을 가지고 있는 인간의 모든 행동을 포함하는 것이다. 이러한 개념에서 본다면, 운전원의 정상적인 행동 및 절차서에 입각한 정상적인 직무조치라고 하더라도 시스템에 부정적인 결과를 초래할 경우에는 인적오류로 분류해야 한다(장통일 등, 2002). 독립적으로 볼 때에는 정상적인 기능을 위한 행위라고 해도 최종적으로 시스템에 부정적인 영향을 끼치거나 그러한 가능성을 가지는 경우에는, 인적오류로 분류하거나 인적오류의 일부분(segment)을 구성하는 것으로 분석과정에 포함하였다. 그림 2에서 보는 바와 같이 기기의 동작이나 사용자 반응의 모든 가능한

2.2 분석 절차

2.2.1 오류절편(Error Segment)

위에서 제시한 시스템 안전 측면에서의 기본개념을 도입한 결과, 그림 3과 같이 기기와 사용자에게 대한 영향관계의 파급을 나타낼 수 있는 기본적인 표현방식을 제안하였다.

기본구성	기능 (function)	영향요인 (causal) factor	변화된 기능 (failure)	영향 (effect)	오류절편 (Error Segment)
기계	기능 (Function)	외부요인	문제발생 (Problem)	영향 (Effect)	ES _M
인간	반응 (Response)	외부요인	문제발생 (Problem)	영향 (Effect)	ES _H

그림 3. 오류절편(Error Segment: ES)의 개념

원전에 부정적인 결과를 야기할 수 있는 가능성을 가진 기본 단위는 기능, 영향요소, 변환된 기능, 효과 등으로 구성되는데, 이를 오류절편(Error Segment : ES)이라고 정의하였다. 오류절편에서 기능(function)은 기기의 경우, 기기가 가지는 고유의 설계특성 및 기능

을 말하며, 인간의 경우에는 MMI 조작행위를 나타낸다. 영향요소(influencing factor)는 동작이나 행동에 대하여 원인이 되는 요소를 말하며, 변환된 기능(changed function)은 이러한 영향요소들에 의하여 야기된 기본 기능의 변화, 특히 결함이나 고장(failure)을 나타낸다. 마지막으로, 영향효과(effect)는 일련의 오류절편의 내부 과정에 의하여 발생하는 결과적인 상태를 나타낸다.

기기와 관련 오류절편(ES_M)은 기기가 가지는 고유의 설계특성이나 기능이 특정한 외부 요인에 의하여 문제가 발생하게 되면 그에 따른 효과가 표시된다. 한편, 인간과 관련된 오류절편(ES_H)은 기기의 기능에 해당하는 부분이 외부의 정보에 대한 반응으로 나타나고, 그러한 반응이 특정 요인에 의하여 부정적인 문제로 발현되고 최종적인 효과가 발생한다.

위와 같은 상호작용의 과정을 ES로 표현하면, 시스템의 고장은 이러한 ESi들의 연쇄과정인 {ESi}에 의하여 발생하게 된다. 즉, 단일 ES는 복수의 ES들을 야기할 수 있고, 연쇄적으로 많은 ES들을 야기할 수 있다. 이러한 ES들의 결합으로 표현되는 연쇄작용 중에서 시스템에 바람직하지 못한 쪽으로 진행되는 집합은 결국 시스템에 부정적인 영향을 주는 인적오류로 귀결된다.

이러한 원리는 이미 시스템의 안전성 평가 기법으로서 널리 이용되고 있는 FMEA와 유사한 절차를 따르고 있다. 차이점이 있다면, FMEA의 경우에는 ES_M에 해당하는 기기관련 오류절편만을 대상으로 분석하지만, 본 연구에서는 ES_H을 중심으로 오류절편을 도출한다. 또한, ES_H뿐만 아니라 ES_M와의 상호작

용이 발생하는 경우에 대하여 집중적으로 분석한다. 확장된 인적오류 개념과 동적인 분석 과정을 채택하고 있는 것이 특징이다.

2.2.2 분석 절차의 구성

제안된 분석절차의 기본적 구조는 안전성 분석에서 널리 쓰이는 FMEA과정을 인적오류 분석에 접목한 것이다. 그림 4는 FMEA를 기반으로 MMI 설계를 지원하도록 제안된 분석 절차를 흐름도로 나타낸 것이다.

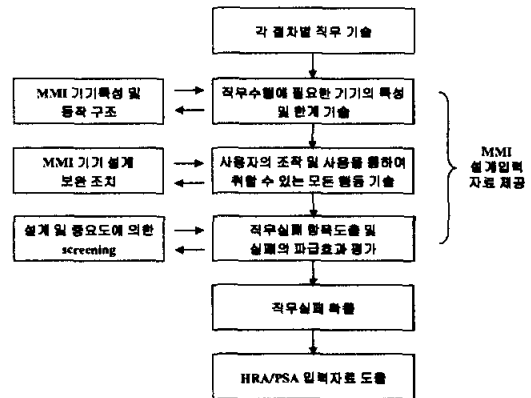


그림 4. 기법의 분석절차

즉, 특정단계의 절차에서 수행해야 할 직무를 세분하고, 그러한 직무를 수행하기 위하여 조작하여야 하는 기기에서 발생가능한 기기의 특성이나, 한계를 반영한 다양한 상태를 열거하였다. 그리고 그러한 특성과 한계 때문에 운전원이 기기에 대해서 조작 및 사용을 통해 취할 수 있는 모든 상호작용 행위를 기술하였다. 결국, 이러한 결과는 기기의 특성에 기인하여 발생 가능한 인적오류들을 차례로 열거하는 상호작용 평가 혹은 Human-FMEA의 일종이라고 할 수 있다. 기기 또는 운전원의

기본기능이 어떤 요인에 의하여 변화될 수 있는 목록을 FMEA의 기본적인 도표와 유사한 형식으로 정리하는 것이다.

2.2.3 정량화와 Screening

최종적으로 시스템에 유의한 영향을 미치는 것으로 판단되는 오류절편의 연쇄군들은 HRA를 위한 정량적인 평가의 대상이 된다. 도출된 오류항목들의 발생 가능성에 대한 정량화(quantification)는 오류절편의 각 연결 부위에 대한 조건부 확률을 결합하여 얻는다.

정량화는 다음 표 1에서 보는 바와 같은 정량화 기준에 따라 1.0, 0.5, 0.1, 0.01, 0.001, 0.0001 등 6가지 수준의 명목치(nominal value)를 부여하는 방식으로 평가한다. 이는 전체 HRA 과정은 물론 MMI 설계자들의 판단과 결합하여 중요하지 않은 오류 항목들이 screening되는 과정을 반복적으로 거치도록 제안된 것이다. 오류절편에 의한 정성적인 분석 결과를 전체 안전성 판단에 결합하여 다른 분야에서 쉽게 이해하고 활용하는 과정으로 필요하다.

표 1. 조건부 확률의 명목치 및 할당기준

명목치	조건부 확률의 할당기준
1.0	항상 발생하는 경우
0.5	대부분의 경우 발생 가능한 것으로 인식되는 경우
0.1	발생 가능성이 일부만 인정되는 경우
0.01	발생 자체는 가능하지만, 확률은 낮다고 보이는 경우
0.001	가능한 오류이나 발생확률이 거의 없는 경우
0.0001	전혀 발생할 수 없는 경우

계산방법은 그림 5와 같은 예를 통하여 확

인할 수 있다. 첫 번째 단계로 시스템의 고장을 야기할 수 있는 모든 오류절편의 연쇄관계를 나열한 다음, 오류절편의 연쇄 효과가 시스템의 한계를 초과하는 것들만을 선별한다. 즉, 최종 효과가 시스템의 한계를 초과하여 오류라고 판명된 오류절편들에 대한 확률값을 취하고, 충분히 작아서 그 발생확률을 무시할 수 있는 연쇄는 분석과정에서 제외한다. 마지막으로 선별된 오류절편의 연쇄들의 곱으로 계산하여 최종적인 오류확률을 구한다.

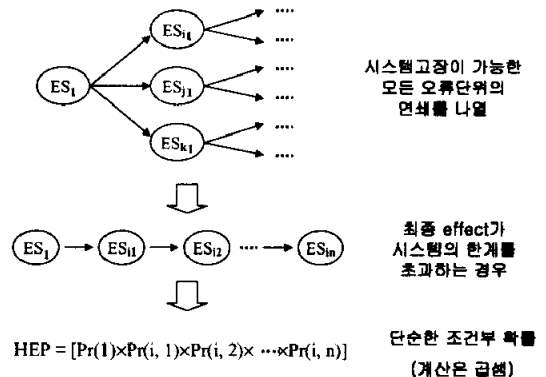


그림 5. 오류절편에 대한 확률 계산방법

제안된 정량화 방법은 개괄적인 명목치를 사용하지만 분석의 실무를 위한 screening 과정을 병행하는 방법이다. 명목치 부여는 새로운 기기의 설계에 대한 세부적인 상호작용의 가능성이므로, 기존의 확률자료가 존재하지 않는다. 따라서, 현재로는 오류 가능성에 대한 전문가 집단의 합의에 의한 평가만이 가능하다. 하지만, 분석이 필요한 가능한 경로를 줄여주어 제안된 기법을 실무적으로 가능하게 하기 위하여 반드시 필요하다.

3. 적용결과

3.1 원전 제어실 설계

앞에서 밝힌 바와 같이, 차세대 원전의 주 제어실 인터페이스는 기존 원전의 주 제어실과는 전혀 다른 형태 및 기기들로 설계되고 있다. 원전의 전체적인 상태를 감시할 수 있는 대형 표시장치, 세부항목의 감시 및 제어를 가능하게 하는 개인용 모니터 등 전형적으로 전산화된 작업환경을 채택하고 있으며, CRT 나 LCD, touch screen, 마우스 등과 같은 MMI 기기들로 구성되어 있다.

따라서, 제어반의 다양한 표시기를 통하여 제공되었던 거의 모든 정보들이 간단한 화면을 통하여 운전원들에게 제공되고, 또 그러한 정보에 대한 제어 및 원전에 대한 제어조작도 마찬가지로 화면 조작을 통하여 피드백(feedback)이 이루어진다. 그렇기 때문에 이러한 화면표시장치 및 관련 조작기와 관련된 기기의 결합 및 인적오류에 대한 대비가 가장 중요한 설계 현안의 하나로 부각되었다.

화면표시장치와 관련된 오류가능성을 평가하기 위해서 먼저 기기의 동작 및 기기 동작과 관련하여 발생 가능한 운전원의 행위에 대한 독립적인 분석이 필요하다. 파악된 기기의 동작 및 운전원 행위들은 각각 일정한 영향을 일으키는데, 이들은 개별적인 오류절편을 구성한다. 오류절편에서는 여러가지 영향들 중에서 FMEA에서와 유사하게 부정적인 조치 혹은 상태들을 모두 열거하였다. LCD의 도입과 관련하여 다음 표 2는 기기의 동작을

유형별로 분류한 것이며, 표 3은 가능한 운전원 조작의 분류 결과를 나타낸 것이다.

표 2. 기기의 동작 분류 : LCD(예)

기기기능	가능한 기기 기능의 범위
정보 표시	기기의 과밀표시
	icon의 유사성으로 인한 구분 안됨
	sensitivity 및 precision 부족
	실제 시스템과의 양립성 결여
화면정보 freeze	
정보 처리	정보획득시간 과다(지연)
	반응시간 지연
기기 변경	(기기의 외형적인 기능 변경 동작)
화면 변경1	화면 update
	CRT 표시상 navigation 요구
	page분할(subsystem-component)
화면 변경2	색채
	문자

표 3. 운전원의 조작행위 분류 : LCD(예)

행위항목	가능한 세부 조작행위의 범위
정보검색	관련정보 활용
	획득 추가조치
	다른 기기의 조작요구시 검색 누락
정보의 전달	조치의 누락/실패
기기변경 (변경1)	CRT와 system의 power On/Off 조작
	창을 여닫는다
화면변경 (변경2)	다른 기기화면 참조
	표시변경시도 (추가작업)
	다른 정보표시 활용 (회복보완조치)
정보입력	조치의 누락/실패
	기기 조작 오류
	중복조작시도 및 그에 의한 조작누락
	조작오류
	착오조작
오조작 및 선택오류	

MMI 기기별로 조작방식이 동일하므로 분석과정에서 적용되는 오류절편은 기본적으로 일정하나 직무의 세부성격에 따라 조정된다. 따라서, 직무분석을 통하여 직무유형별로 고려되는 오류절편 및 조합을 조정한다.

표 4. AFWP의 절차에 따른 발생가능 오류의 분류(일부)

절 차	operation	발생가능한 동작 및 행위	
		기기 동작	운전원 조작행위
1.0 AFWP 탐색 및 이동	AFWP 구동을 위한 화면 탐색 (정보활용)	기기의 표시 (과잉) 실제 시스템과의 양립성 결여	유사한 위치의 다른 기기 검색 다른 기기 화면 참조
	AFWP click (정보입력)	화면정보 freeze 반응시간 (지연) icon의 유사성 및 기기의 혼동요소	CRT 및 시스템의 전원 On/Off 조작 재조작/중첩조작 선택 (오류)
1.1 P/P 구동			
(1) HS-009A P/P			
a. HS-009A P/P 구동	HS-009A 탐색 (정보활용)	icon의 유사성 및 기기의 혼동요소	선택 (오류)
	HS-009A click (정보입력)	화면정보 freeze 화면정보 표시 (지연)	CRT 및 시스템의 전원 On/Off 조작 재조작/중첩조작
	pop-up 창 open		
	HS-009A 구동조작 (정보입력)	화면정보 freeze 화면정보 표시 (지연)	CRT 및 시스템의 전원 On/Off 조작 재조작/중첩조작, 착오조작 (타작업조작), 기기조작 (실패/누락)
b. HS-045A VLV open	HS-045A 탐색 (정보활용)	icon의 유사성 및 기기의 혼동요소	선택 (오류)
	HS-045A click (정보입력)	화면정보 freeze 화면정보 표시 (지연)	CRT 및 시스템의 전원 On/Off 조작 재조작/중첩조작
	pop-up 창 open		
	HS-045A open 조작 (정보입력)	화면정보 freeze 화면정보 표시 (지연)	CRT 및 시스템의 전원 On/Off 조작 재조작/중첩조작, 착오조작 (타작업조작), 기기조작 (실패/누락)

3.2 급수상실사고의 인적오류 평가

3.2.1 오류절편 항목 도출

MMI 기기 관련 오류절편들에 대한 조사 결과를 이용하여 원전의 급수상실사고(Loss of Feed Water)중 보조급수계통(Auxiliary Feed Water System)의 작동실패 가능성을 검토하는 데 적용하여, 기법의 기술적인 타당성과 함께 실용적인 응용력을 검토하였다.

급수상실사고란 비상운전시 보조급수계통이 가용하지 않을 경우, 원자로 정지에 따른 열 제거의 실패로 노심의 손상이 야기될 가능성이 있는 시나리오의 하나로 원전의 안전성 평가에서 중요하므로, 오류가능성을 세밀하게 검토한다. 평가결과는 표 4와 같다.

표 4에 나타난 항목들은 기존의 HRA에서는 단순한 조작 실패 확률 이외에는 전혀 포함되지 않았던 것들이다. 또한, 개별적으로는

직접 조작오류나 고장이 아닌 것도 포함되었다. 단순히 하나의 조작 혹은 반응만으로는 매우 사소하며 문제가 되지 않지만, 궁극적으로 시스템에 유의한 오류로 진행되어 급수상실 사고를 야기할 수 있는 것으로 평가되었기 때문이다.

3.2.2 오류절편 도출 및 확률계산의 예

위의 표 4로부터 오류절편들의 연쇄군들을 도출하여 인적오류 확률을 계산하였다. 대부분의 경우, 최종적인 확률값은 안전성 평가에서 제외될 수 있을 만큼 충분히 낮았으므로 HRA에서 영향은 미미하였다. 그러나, MMI 설계와 관련하여 안전성 측면에서의 보완이 필요한 설계항목을 도출하였다. 예를 들면, 표 5와 같이 인적오류확률을 정량화함으로써 표시기로서의 LCD의 설계에서 표시반응의 지연 방지 및 지연시 재조작 차단 필요성과 그 정성적인 효과를 도출하였다.

표 5. 오류절편 및 발생확률의 예

연쇄단계	0	1	2	3	4
	조작	기기	인간	기기	인간
오류절편	AFWP click (정보입력)	반응시간 (지연)	재조작/ 중첩조작	화면정보 표시 (지연)	착오조작 (타작업 조작)
조건부 발생확률	→	→	→	→	
	0.5	0.5	0.5	0.1	

위 표에 나타낸 예는 보조급수계통 관련 운전 절차 1.0에 해당하는 'AFWP 탐색 및 이동' 절차로서 첫 번째 단계에서 AFWP를 구동하기 위한 클릭이라고 하는 조작행위의 입력이 발생한다. 이러한 조작행위 후의 기기의 오류반응으로는 반응시간의 지연이 발생 가능하다. 2단계에서는 기기의 반응시간 지연으로 인하여 운전원은 재조작 및 중첩조작이라고 하는 특유의 조작행위가 발생한다. 즉, 반응에 대한 피드백이 즉시 나타나지 않으면, 운전원은 클릭이라고 하는 조작행위를 재입력하게 되는 것이다. 매우 간단하지만 3단계에서는 선행의 기대되지 않은 행위에 의해 다른 반응이 입력될 수 있고, 그 결과 화면정보표시의 지연이 발생할 수 있는 것으로 분석되었다. 4단계에서는 화면의 정보표시 지연에 의해 이미 해당작업을 수행하였음에도 불구하고, 동일한 작업을 반복 수행하거나, 임의의 다른 작업을 수행할 가능성이 발생한다.

한편, 표에 나타난 각 단계의 발생확률은 이미 앞에서 언급하였던 조건부 확률의 명목치 할당기준에 의하여 결정된 값으로서, 위의 예에 나타낸 시스템 오류의 발생확률은 각 단계의 오류절편들의 확률값의 곱($0.5 \times 0.5 \times 0.5 \times 0.1$)인 1.2×10^{-3} 이다. 확률값으로 판

단하였을 때, 보조급수 펌프 작동 실패라는 오류 발생은 가능하지만, 확률이 충분히 낮은 경우가 된다. 그러나 확률값은 낮다고 하더라도 오류의 파급효과를 방지할 수 있는 방안이 충분히 마련되어 있지 않은 경우에는, 그 파급 영향을 그대로 수용하기에는 위험성이 높다. 따라서, 표시반응의 지연 방지 및 표시 지연시 재조작 차단(혹은, bypass) 등 오류절편의 연쇄작용의 진행을 방지할 수 있는 적절한 대안을 각 단계별로 수립하도록 권고하였다.

4. 결론 및 토의

본 논문에서 제안된 인적오류 평가 기법은 시스템 안전 개념을 기반으로 오류절편이라고 하는 새로운 개념을 도입하여 분석함으로써, 기기와 운전원과의 상호작용(interface)에서 발생할 수 있는 오류 가능성에 대하여 기존의 기법들이 가지는 한계를 극복할 수 있는 가능성을 보였다. 또한, 새로운 원전 주제어실 설계에서 급격히 변화하고 있는 MMI 기기의 특성에 따라 유도된 오류(device-induced error) 및 수행오류(EOC) 등 보다 확대된 오류 가능성을 평가 범위에 포함할 수 있도록 하였다. 따라서, HRA 평가에서 필요한 기초 오류확률값 중에서 기존의 기법들에서는 얻기 어려웠던 오류 가능성 항목들의 정량적 평가가 가능하게 되었다. 또한, MMI 기기들의 인터페이스 설계 과정에 직접 활용 가능한 세부적인 평가결과를 도출할 수 있었다.

MMI기기에 대한 오류 가능성의 추적은

ThERP와 유사한 과정이므로 제2세대 HRA 기법들에 비하여 실무에 부담이 없다. 또한, 개별적인 오류절편에 대한 일회적인 평가로 끝나는 것이 아니라, 다른 오류절편으로 연결하는 방식이므로 사소한 요소로부터 파급된 오류나 정상적인 상호작용들이 누적되어 오류로 발전하는 경우를 분석하는데 적합하다.

본 연구에서 제안된 분석 방법은 원전뿐만 아니라 오사용(mis-use) 평가 등 제조물 책임 분야의 제품 안전성(product safety) 평가에서 기존 FMEA가 가진 하드웨어 중심 분석의 한계를 보완하도록 적용할 수 있다.

그러나, 실무와 응용의 확대를 위해서 아직은 몇가지 보완해야 할 부분이 있다. 우선, MMI 기기에 따라 도출되는 개별 오류절편들에 대하여 가능한 반응 유형에 대한 실증적인 조사와 각각에 대한 조건부 확률값의 재조정이 필요하다. 이는 상호작용에 대한 지속적인 기초 조사와 오류절편의 개별적인 실험에 의한 기초 자료 수집으로 보강해야 한다. 둘째, 본 기법의 실무 활용을 위해서는 오류절편들의 누적 및 파급 오류에 대한 효과적인 분석이 가능하도록, 전산화된 동적인 분석지원체계를 보강할 필요가 있다. 오류절편의 연쇄과정을 추적하는 단계에서 수작업의 부담을 덜어주도록 기존의 FMEA 도구를 수정 보완하여 활용하는 방안을 고려할 수 있다.

참고 문헌

김재환, 정원대, 원자력발전소 사고관리 직무의 인간신뢰도분석을 위한 수행영향인자의 선정, 대한인간공학회지, Vol.20,

No.2, pp.1-28, 2001.
 서상문, 이용희, 천세우, 모의 비상운전 시나리오 수행에 따른 운전원들의 인지적 직무특성 분석, 한국원자력학회 추계학술대회, 1995.
 이동하, 이현철, 상황인식에 대한 측정 및 차세대 원자로 운전원 성능 평가에서의 활용방법에 관한 이론 연구, Vol.13, No.4, pp.751-758, IE Interfaces, 2000.
 이용희, 원전에서 전산화 도입으로 인한 인적 오류 가능성 분석의 기본체계, 추계학술발표회, 한국원자력학회, 1999.
 이용희 외, 첨단 제어실 기기 도입을 위한 인적오류 가능성 검토, KINS 첨단 계측 제어 Workshop, 2000, 한국원자력안전기술원, 2000.
 장통일, 이용희, 임현교, 원전의 인적오류(Human Error)에 대한 분석기법의 개발, 한국산업안전학회 추계학술대회 논문집, pp.245-248, 2002.
 정광태, 이용희, 전산화된 작업 환경에서 운전원의 오류 가능성에 대한 기초연구, 대한인간공학회지, 19권 1호, pp.1-9, 2000.
 정원대, 박진균, 김재환, 원자력발전소 비상직무에 대한 인적수행도 분석, 대한인간공학회지, Vol.21, No.3, pp.13-24, 2002.
 CEC, Human Factors Reliability Benchmark Exercise, EUR 12356 EN, 1988.
 Choen, S. W, et. al, Modelling of

Operator's Cognitive Behaviour in Nuclear Power Plants Using Blackboard Techniques, Journal of New Review of Applied Expert Systems, vol.3, pp.81-95, 1997.

Hollnagel, E., CREAM : Cognitive Reliability and Error Analysis Method, 1997.

Kirwan, B., Human Reliability and Safety Analysis Handbook, 1992.

Lee, Y. H., Facilitating HRA through the Input from HSI Design, 2-nd OECD/NEA Workshop on Building the New HRA, 2002.

O'Hara, J. M., et al., Integrated System Validation: Methodology and Review Criteria, NUREG/CR-6393, 1997.

U. S. NRC, Human Factors Engineering Program Plan, NUREG-0711, 1994.

U. S. NRC, Technical Basis and Implementation Guidelines for ATHEANA, NUREG-1624, 1998.

Yoon, W. C. and Lee, Y. H., A Model-based and Computer-aided Approach to Analysis of Human Errors in Nuclear Power Plants Reliability Engineering and System Safety, vol. 46, pp.43-52, 1996.

저자 소개

◆ 이용희

1983년 서울대학교 원자핵공학과 졸업

1985년 서울대학교 대학원 산업공학과 졸업

현재 한국원자력연구소 인간공학실 근무

관심분야 : 인적오류, 인터페이스 설계 및 평가, 인지 시스템, 안전성 평가

◆ 장통일

1997년 충북대학교 안전공학과 졸업

1999년 충북대학교 대학원 안전공학과 졸업

현재 충북대학교 안전공학과 박사과정

현재 한국원자력연구소 인간공학실 근무
관심분야 : 인적오류, 안전성 평가, 작업 피로도

◆ 임현교

1982년 서울대학교 산업공학과 졸업

1984년 한국과학기술원 산업공학과 졸업

현재 충북대학교 안전공학과 교수

관심분야 : 산업안전, 제품안전, 인적오류

논문접수일 (Date Received): 2003/01/26

논문게재승인일(Date Accepted): 2003/02/10