비상사고 시 운전원의 부적절한 조치 가능성에 대한 사례검토 및 분석 방향

A Framework for Analysing Human Errors of Commission in Emergency Situation

김재환, 정원대, 박진균
한국원자력연구소
대전광역시 유성구 덕진동 150번지

요 약

TMI-2 사고 이후 원전 운전원의 부적절한 조치(EOC: Errors of Commission) 가능성에 대한 관심이 증가되어 왔고, 원전 위험도 분석에도 이러한 EOC 사건을 고려하여야 한다는 의견이 제기되고 있다. 본 연구에서는 이러한 추세에 따라 미국의 주요 원전 사건/사고에서 개입되었던 운전원의 부적절한 조치 사건을 검토하고, EOC 유형과 이를 유발하게 된 상황 및 내재 요인을 정리하였다. 또한, EOC 사건에 대한 분석 결과를 바탕으로 원전 위험도 분석 체계 내에서 EOC 사건을 분석할 수 있는 분석 체계를 제시하였다. 제안한 분석 체계에 따라 고리 3,4호기의 일반과도사건에서 고려될 수 있는 EOC 사건을 도출하였다.

Abstract

Since the TMI-2 accident, interest in human errors of commission (EOC) that is inappropriate actions committed by human operators has been increased, and furthermore, it has been raised among risk analysts that these EOC events should be incorporated in risk assessment of nuclear power plants (NPPs). According to this trend, this study reviews several EOC events that have intervened in NPP events/accidents of USA, and analyses the type of EOC and contextual factors and latent conditions related with each event/accident. Based on this review, a framework for analyzing EOC events is introduced to identify and analyse important EOC events for inclusion into risk assessment. In addition, important EOC events appearing in the general transient event of the Kori 3&4 NPPs are presented.

1. 서 론

1979년에 발생한 미국 TMI-2 원전 사고는 원전 사건 및 사고의 발생과 전개에 있어서 인적행위가 극히 중요한 기여요소로서 작용하고 있다는 것을 보여주고 있다. TMI-2 사고대응 과정에서 드러난 대표적인 운전원 관련 조치는 발전소의 물리적 상태는 안전주입이 필요한 상태이나 운전원의 상황판단 오류로 말미암아 작동 중인 안전주입계통을 장시간 동안 정지시킨 것이다. 이러한 운전원의 행위는 발전소의 특정한 물리적 및 환경적 상황에서 요구

되는 조치 외에 상황에 부적절한 조치를 수행하여 발전소의 안전상태를 악화시킬 수 있는 가능성이 존재한다는 것을 보여 주었다. 이러한 발견은 TMI-2 후속조치로서 PORV를 포함한 기기 설계변경과 절차서 및 훈련과 같은 운전원 지원 시스템의 개선과 아울러, 원전 위험도 평가 방법에 있어서의 개선 필요성도 인식되었다.

원자력발전소와 같은 대형 시스템의 안전성을 평가하는 기법으로서 확률론적 안전성 평가 (PSA: Probabilistic Safety Assessment) 기법이 활용되고 있다. PSA는 다양한 초기유발사건으로부터 시작하여 시스템의 회복 불가능한 상태에 도달하기까지 발생 가능한 모든 사고경위를 예측적으로 분석하고, 각각의 사고경위의 발생 가능성을 확률적으로 계산하고 이를 합산하여 전체 사고발생확률을 구하는 방법이다. 사고경위에는 각 초기사건에 대하여 필요한 기기의 기능실패와 인적행위의 실패 모두를 포함하고 있다. PSA 기법의 적용을 통해 모든 예상 가능한 사고발생 경로와 함께 기기 및 인적행위를 포함하는 취약한 사고경위를 파악함으로써 사고발생 감소를 위한 적절한 조치를 효율적이고 효과적으로 취할 수 있게 된다.

PSA 기법 내에서 파악된 사고경위 중 인적행위의 실패 가능성을 평가하는 부분을 인간신뢰도분석(HRA: Human Reliability Analysis) [Dougherty, 1988] 방법이 담당하고 있다. HRA에서는 인적오류유형을 크게 EOO(Errors of Omission)와 EOC(Errors of Commission)로 분류하고 있다. EOO는 누락오류로서 운전원에게 요구되는 직무를 주어진 시간 내에 완료하지 못하는 것을 뜻하며, EOC는 운전원의 조치가 주어진 상황에서 부적절한 조치인 오류사건을 나타낸다. 그러나, 현재 원전 PSA에서 고려되는 인적오류사건의 범위는 대부분 EOO로 제한되어 있으며, TMI-2에서 발생한 안전기기의 종료와 같은 부적절한 조치 행위는 고려하고 있지 못한 상태이다. 그러나, TMI-2 원전 뿐만 아니라 그 이후의 여러 원전에서도 TMI-2와 유사한 EOC 행위가 발생됨에 따라, EOC의 원전 위험도 분석에의 포함에 대한 필요성이 많은 안전성 분석가들에 의해 인식되고 있다 [Hollnagel, 2000; OECD/NEA, 2001].

EOC 분석 방법에 대한 연구는 미국 Maryland 대학의 Mosleh 교수 팀에서 이루어진 Macwan [Macwan, 1994] 및 Julius [Julius, 1995]의 분석 방법 및 절차에 대한 소개가 있었고, PSI에서 Davis-Besse 사건에서 개입된 EOC 사건을 이용한 사례적용[Reer, 1999]과 Swiss 원전에서의 시범 분석/평가가 소개되었다 [Dang, 2001]. 최근에는 원전 사례분석을 통한 광범위한 인적오류사건을 다루고 있는 미국 NRC에서 개발한 ATHEANA [USNRC, 2000] 방법이 제시되었으나, 상당한 분석 자원의 요구로 인해 원전 위험도 평가체계에서의 활용성에는 많은 제약이 있을 것으로 평가되고 있다.

본 연구에서는 이러한 연구 추세에 따라 국내 원전의 위험도 분석에의 고려를 위한 EOC 분석 방법을 개발하기 위한 첫 번째 시도로서 먼저, 미국 원전에서 발생한 기 발생 사건을 검토하여 이들 사건에서 발생한 EOC의 유형과 상황요인들을 정리하였다. 또한, 검토 결과를 바탕으로 하여 위험도 분석을 위한 EOC 분석 체계를 제시하고, 이 체계에 따라 고리 3,4호기 원전에서 고려될 수 있는 대상 EOC 사건을 도출하였다. 제2절에서 기발생 사건

에 대한 EOC 사건 검토 결과를 정리하였고, 제3절에는 위험도 분석에의 고려를 위한 EOC 분석 체계를 제시하고, 제4절에서 고리 3,4호기 일반과도사건에서 고려될 수 있는 EOC 사건들을 정리하였다.

2. 기발생 사건의 EOC 사건 검토

미국 원전에서 발생한 주요 사건 중 원자로 정지 후 대응과정에서 EOC 사건을 포함하고 있는 사건들을 관련 문헌들을 통해 검토하였다. 검토한 문헌은 ATHEANA [USNRC, 2000]의 인적오류 사건 사례분석 자료를 기반으로 하고 있으며, 각 사건에 대한 상세 자료는 참고문헌 [USNRC, 1985], [USNRC, 1993], [Dougherty, 1998] 등을 참조하였다. 각 사건별로 발생한 인적오류사건과 발생 원인을 요약하고, 주요 내용을 표 1에 정리하였다.

TMI-2: Loss of MFW & PORV Stuck Open, 1979

TMI-2 사고에서 개입되었던 운전원의 EOC 사건은 TMI-2 원자로를 노심 용융으로까지 이르게 했던 결정적인 사건으로 평가되고 있으며, 이 사건으로 원전 운전원의 부적절한 조치 가능성에 대한 연구가 관심을 끌기 시작했다. 작업자 실수로 인한 주급수 계통의 운전정지와 보수 작업자의 밸브 닫힘 상태 방치로 인한 보조급수의 약 8분간의 급수 실패로 인하여 원자로 내의 고온/과압이 발생하고, 이로 인해 가압기 압력방출밸브(PORV)가 개폐 작동을 시작하게 된다. 그러나, 개방 작동된 PORV가 닫힘 작동에 실패하고 PORV를 통해 냉각수가 방출되는 PORV LOCA가 사건진행 도중 추가적으로 발생한다. 원자로 압력이 고압안전주입계통(HPSI)의 작동 설정치 이하가 되어, HPSI 계통이 자동적으로 작동되고 있었으나, 이 시점에서 TMI-2 운전원은 발전소 상황에 대한 오판단으로 운전중인 HPSI 펌프를 중단시키게 되는 중대한 EOC 조치를 취하게 된다. 이 조치와 관련한 EOC 유형(ATHEANA 분류체계)과 이를 유발하게 된 주요 상황 및 내재적 요인을 정리하면 다음과 같다.

EOC 유형:

- Human Failure Mode: Equipment (HPI) inappropriately terminated.
- Unsafe Action: Operators stop equipment (HPI)

상황적 요인:

- 물리적 상황: PORV 개방 고착으로 인한 원자로 냉각수 방출
- 계측 정보:
  - 가압기 수위: 고수위 지시
  - PORV 상태 지시계: 닫힘 상태 지시 (실제상태를 계측한 정보가 아닌 제어신호를 지시하도록 설계됨 -> 설계오류)
  - PORV 온도 지시계: 고온 지시
  - 음향 신호: 작동중이었으나 MCR back panel에 위치
- 절차서: PORV LOCA에 대한 상황판단 및 조치 사항이 없었음.

- 훈련:
  - PORV Stuck-open 가능성에 대한 학습 및 훈련 부재
  - 가압기 만수위 방지에 대한 주의

결론적으로, TMI-2 사고는 운전원의 조치를 요하는 증상을 띠는 물리적 현상의 전개와 계측 정보의 오류가 결합되어 발생한 운전원의 상황판단의 오류로부터 발생되었다고 볼 수 있다. 또한, 계측 정보 상으로는 발전소에 대한 운전원의 초기 상황모델을 수정시킬 수 있는 정보들이 존재하였음에도 불구하고, 경험 및 훈련 부재와 잠재적 문제로 인하여 무시되었던 점은 여러 오류분석 전문가들에 의해 주목을 받고 있다 [Reason, 1990; USNRC, 2000].

Davis-Besse: Loss of MFW, 1985

1985년 Davis-Besse 발전소에서도 TMI-2와 유사한 사건이 발생했는데, 주급수계통 상실사건으로 원자로 정지가 발생한 후 증기발생기의 수위가 감소되는 것을 확인한 운전원이 보조급수계통이 자동으로 작동할 것을 예상하고 미리 이 계통(보조급수계통)을 수동으로 작동시키려 하는 중 부주의로 이 보조급수계통을 차단시키는 밸브를 누르는 오류를 범한다. 다시 복구하려는 시도를 하지만 밸브 구동 관련 보정이 잘못되어 있음으로 인하여 재기동에 실패하게 되고, 현장 운전원을 통한 복구 작업이 지시된다. 주급수 상실 후 보조급수 상실이 연이어 발생하게 되어 원자로 고압력으로 인한 PORV 개폐 작동이 시작되고, 순간적으로 개방 고착되었으나 다시 닫힘 상태로 복구된다. 이러한 시점에서 원전 비상운전절차서에 의하면 방출 및 주입(feed & bleed)을 수행하도록 지시되어 있으나, 운전 팀은 보조급수계통의 복구를 예상하고 방출 및 주입 조치를 유보한다. 결국, 운전 팀의 예상대로 보조급수계통의 복구가 이루어지고 발전소는 안정 상태로 유지된다. Davis-Besse 사건에 개입되었던 중요한 인적오류사건은 표 1에서와 같이 두 개로 요약된다. 이 중 두 번째 오류사건은 EOO (누락오류) 유형의 오류이므로 첫 번째 오류사건에 대하여 정리하면 다음과 같다.

EOC 유형:

- Human Failure Mode: Equipment (AFW) inappropriately isolated or aligned.
- Unsafe Action: Operators realign equipment (AFW)

상황적 요인:

- 물리적 상황: 주급수 상실 후 보조급수 주입이 요구되는 시점
- 운전원 훈련 정책: 자동 작동이 긴급하게 요구될 시 우선 수동 작동 권고
- 정보 시스템: 스위치 배열의 혼동 가능성
- 잠재적 오류: 보조급수 차단 밸브의 오보정 상태

Davis-Besse 발전소의 EOC 사건은 TMI-2와는 달리 단순 수행오류(execution error)로 인해 발생되었으나, 보조급수 차단 밸브의 오보정 상태와 같은 잠재적 문제와 결합함으

로써 인적오류 행위 자체의 복구는 불가능하게 되었다.

Fort-Calhoun: Loss of Electrical Fault, 1992

전기계통인 인버터의 전압 불안정으로 인해 전원 단절이 발생하고 터빈제어밸브가 닫힘으로 인하여 RCS의 열제거원이 상실되다. 이로 인해 RCS 내부의 온도 및 압력이 상승하게 되어 원자로가 정지되고, 이어 가압기 방출밸브(PORV) 및 안전밸브(PSV)가 개방 작동된다. 이후 압력이 감소되면서 PORV는 다시 닫힘 상태로 복구되었으나, PSV는 초기의 압력상승으로 인해 설정치가 감소되는 현상이 발생하여 일부 개방되어 있는 상태가 지속되었다(PSV LOCA 발생). 이러한 사건에 대해 Fort-Calhoun 운전팀은 비상운전절차서의 진단절차를 이용하여 '복합 사건'으로 진단하고 회복 절차서로 전이를 결정한다. 그러나, 압력 설정치 만족으로 안전주입은 작동되고 있었으나, 절차서 진행 중 'HPSI 종결조건'에 이르러 상황에 적절치 않은 'HPSI 유량 감소 조치'를 취하게 된다. 이러한 조치를 취하게 된 근본적인 원인은 'HPSI 종결조건' 중의 하나인 'RCS 과냉각도'로 인한 것인데, 사건진행 당시 가압기 압력 계기는 실제 압력보다 어느 정도 높은 상태로 실제 압력의 추이를 따라가고 있었기 때문에 실제보다 RCS 과냉각도가 충분히 만족하는 것으로 오인되었다. 가압기 압력 계기와 관련하여 다른 두 개의 다중 계기가 존재하고 있었으나 back panel에 위치하고 있음으로 인해 확인이 용이하지 않았고, 또한 STA(Shift Technical Advisor)를 통해 SPDS 상에서 한 계기가 다른 두 계기와 차이를 보이고 있음을 통보 받았으나 SPDS에 대한 신뢰성 및 팀 조직 상의 문제로 인해 수용되지 않았다. Fort-Calhoun의 EOC 사건유형과 개입된 상황요인을 정리하면 다음과 같다.

EOC 유형:

- Human Failure Mode: Equipment (HPI) inappropriately terminated.
- Unsafe Action: Operators stop equipment (HPI)

상황적 요인:

- 물리적 상황: HPSI 작동 후 HPSI 종결조건에 대한 확인 중
- 정보 시스템:
  - 가압기 압력 계기의 고장 (fail high)
  - 가압기 압력의 다중 계기에 대한 설계 결함
  - SPDS에 대한 신뢰성 부족
- 팀 요소(팀원간의 결합력): STA에 대한 신뢰 부족

본 사건은 TMI-2와는 달리 사건 초기에 발생한 PSV LOCA에 대한 사건 진단이 적절히 이루어졌고, 절차서를 이용한 사건 대응이 절차서를 기반으로 잘 이루어진 경우라고 볼 수 있다. 한편, 본 EOC 사건에서 얻을 수 있는 유용한 정보는 다른 백업 정보(redundant or diverse indicators)에 대하여 실제 운전원의 관점에서 가용성과 유용성을 점검하여야 한

다는 것이다. 뿐만 아니라, 여기에는 발전소 운영상의 여러 문제가 포함되어야 할 것으로 본다.

North Anna 2: Failure of Voltage Regulator, 1993

North Anna 2에서는 발전기 계통의 문제로 터빈 정지 및 원자로 정지가 발생한다. 사건 초기에 주급수(MFW) 및 보조급수(AFW) 펌프는 모두 운전 중이었으나, 주급수 계통은 원자로 저온 상태로 인해 차단된 상태로 응축기로 순환 운전 중이었고 보조계통은 3 트레인 모두 자동 운전으로 증기발생기로 급수 중이었다. 이 때 발전소 운전원은 RCS 평균 온도가 감소하는 것을 보고 과냉각(excessive cooldown)을 우려한다. 한편, 이러한 사실을 파악한 BO(Backboard Operator)는 AFWS의 유량을 특정값 이하로 감소시킬 수 있는 상태인 것을 알리고, AFWS을 정지시키고(secure) MFW를 이용할 것을 제안한다(이때, 증기발생기 수위는 저-저 수위 이하임). 이에 대해 상위 의사결정자들은 AFWS의 유량 감소(secure)를 허용한다("secure AFWS"에 대한 의미를 서로 달리 받아들인 것으로 판단됨). 이에 BO는 특별한 통보없이 MFW 우회밸브를 개방시켜 증기발생기에 유량을 공급하고 AFW 펌프를 pull-to-lock 시켜버린다(Disabling of AFWS). 이것은 Engineered Safety Features의 기능을 제거해 버린 결과로서, 만약 주급수 계통에 문제가 발생할 경우 보조급수계통의 자동작동이 실패하게 된다.

EOC 유형:

- Human Failure Mode: Equipment (AFW pump) inappropriately removed from automatic control.
- Unsafe Action: Operators take equipment (AFW pump) out of armed or standby status.

상황적 요인:

- 물리적 상황: 노심 과냉 우려, 주/보조급수 모두 가용함, 보조급수계통에 대한 신뢰성 우려
- 훈련/교육: ESF에 대한 주의 부족
- 의사 소통:
  - 운전원 간 팀 의사소통의 결여
  - 'Secure AFWS'에 대한 의미의 상이한 해석

위 사건은 원전의 비상운전 하에서 운전원이 과냉을 지나치게 우려하여 증기발생기 수위가 저-저 수위 임에도 불구하고 AFWS을 ESF로부터 제거하는 조치를 취하였다는 점에서 주의를 끈다. 또한, 운전원의 안전의식 또는 안전개념에 대한 검토가 필요함을 시사한다.

표 1. 원전 사건/사고에 나타난 주요 인적오류 사건분석 요약

Event Identifier	Plant State	Plant Type/ Vendor	Event Type	Multiple Failures	Instrumentation Failure	Important Human Error Events
TMI-2 (1979)	Full-power	PWR/B&W	PORV LOCA with Loss of MFW	Loss of AFW, PORV stuck-open	PORV indication failure (design problem)	- Inappropriate termination of HPI (EOC; wrong situation assessment)
Davis-Besse (1985)	Full-power	PWR/B&W	Loss of MFW	Loss of AFW, PORV stuck-open	PORV indication failure	- Inadvertent isolation of AFW (EOC; slip) - Intentional omission to implement F&B (EOO; violation)
Fort Calhoun (1992)	Full-power	PWR/CE	PSV LOCA with Loss of Electrical Fault	PSV partially remained open	RCS pressure indicator fails high, Computer displays malfunctioning	- Inappropriate reduction of HPI (EOC; sit.ass.; indicator problem)
North Anna 2 (1993)	Full-power	PWR/W	Failure of Voltage Regulator	-	-	- Disabling of the entire AFWS (EOC; sit.ass. & res. plan.)

3. 위험도 분석을 위한 EOC 분석 체계

본 절에서는 원전의 위험도 평가체계 하에서 고려되어야 할 EOC 사건을 도출 및 분석할 수 있는 분석체계에 대해 제시하고자 한다. 본 연구에서 고려하고 있는 운전원의 EOC 분석체계에는 사보타지 등 의도적인 부적절 행위는 제외되며, 훈련과 절차서를 바탕으로 사고를 완화 및 종결시키기 위한 노력 중에 발생할 수 있는 부적절한 조치 가능성을 다룬다. 앞의 제2절에서 정리한 바와 같이, 운전원이 EOC 사건을 유발시키는 과정은 상황판단에 있어서의 부적절한 상황모델의 형성, 의사결정 시의 부적절한 결정, 수행 상의 부적절한 행위 등으로 크게 분류할 수 있으며, EOC 사건을 유발시키는 주요 상황으로서는 다중 사건(multiple events)의 발생, 계측기 및 지시계의 문제, 운전원 행위 경향, 절차서, 훈련, 팀 조직의 특성 등 다양한 요소들이 관여하고 있음을 볼 수 있다.

본 연구에서는 이러한 다양한 조건하에서 발생할 수 있는 운전원의 EOC 가능성을 분석하기 위하여 사건 전개 특성과 절차서 수행 특성을 고려하여 다음과 같이 크게 세 가지 유형으로 나누어 정리하였다.

- Case 1 : 초기사건(IE: Initiating Event)의 오진단(misdiagnosis)으로 인한 EOC 가능성
- Case 2 : 초기사건으로 인한 원자로 정지 이후의 사건진행 과정에서 새롭게 유발될 수 있는 사건(절차서 변경 또는 물리적 전개특성의 변화 등 새로운 대처방안이 필요한 사건)으로 인한 EOC 가능성
- Case 3 : 주어진 초기사건과 관련된 절차서 수행 중 발생 가능한 EOC 분석.

각 경우에 대하여 고려하는 주요 분석 내용과 고려 요소들을 정리하면 다음과 같다.

- **Case 1 : 초기사건(IE: Initiating Event)의 오진단(misdiagnosis)으로 인한 EOC 가능성**

이 경우는 원자로 정지를 유발하는 초기사건에 대한 잘못된 진단으로 말미암아 부적절한 대응 절차서를 선택하고 이로 인하여 발전소의 안전 상태를 악화시킬 수 있는 부적절한 조치를 수행할 수 있는 경우를 다룬다. 이러한 초기사건의 오진단 가능성은 오진단 확률과 효과 측면을 모두 만족하는 경우에 한하여 분석의 필요가 요구된다. 즉, 다음 두 가지 조건을 모두 만족하는 사건에 대해 필요하다.

- 초기사건 간 유사한 물리적 특성을 나타내는 경우
- 부적절한 절차서의 선택으로 말미암아 수행되는 직무가 해당 초기사건의 위험도에 부정적 영향을 주는 경우

유사한 물리적 특성으로 인한 오진단 가능성의 분석 과정에는 계측기 오류와 시점의 불일치로 인한 오진단 가능성을 고려한다.

- 계측기 오류
- 시점의 불일치

- **Case 2 : 초기사건으로 인한 원자로 정지 이후의 사건진행 과정에서 새롭게 유발될 수 있는 사건(절차서 변경 또는 물리적 전개특성의 변화 등 새로운 대처방안이 필요한 사건)으로 인한 EOC 가능성**

이 경우는 하나의 초기사건으로 인한 원자로 정지 또는 발전소의 과도사건으로 인한 운전원의 원자로 수동정지 후 사고진행 과정에서 물리적 전개특성이 변화되거나 대응 절차서를 변경하여 대처하여야 하는 새로운 사건이 도입될 때 그 시점에서의 운전원 오류가능성을 분석한다. 새로운 사건이 도입될 가능성이 있는 시점은 열수력분석 결과, 안전성분석 결과, PSA 사건수목(ET: Event Tree) 등의 자료를 토대로 하여 초기사건의 물리적 전개 특성을 분석함으로써 얻을 수 있다. 이와 같이 초기사건 발생 후 새롭게 도입될 수 있는 사건으로는 PORV/PSV Stuck-open LOCA, ATWS 유발 SGTR, MSSV Stuck-open LSSB, 급수공급 완전상실, 주요 기기(HPSI 등)의 오작동 등과 같은 것들이 있을 수 있다. 이 중 주요 기기의 오작동 사건은 현재 PSA 모델에서 고려하고 있지 않은 시스템 고장사건이므로 본 연구에서도 제외한다. 이러한 사건의 발생 가능성이 있는 시점이 파악되면, 새로운 사건 도입에 대한 사건 진단 또는 상황 판단 가능성과 함께 운전원의 EOC 가능성을 분석한다. 이 경우에는 다음과 같이 계측기 오기능의 유무에 따라 별도로 EOC 가능성을 평가한다.

<u>관련 계측기의 정상적 작동 시 (가정)</u>:

1. 운전원의 EOC 조치 가능성 평가
   - 정보시스템을 통해 나타나는 물리적 변수의 거동이 원전 안전성에 영향을 주는 (예: 안전계통을 비가용 상태로 만듦) EOC 조치를 취할 수 있는 근거가 운전원 관점에서 존재하는가?
     - 절차서 및 훈련 검토

- 운전 습성 (기기 보호, 불필요한 작업의 발생 우려 등)

2. 절차서를 통한 사건 진단 및 상황 판단 가능성 평가
   - 해당 발전소의 현 절차서가 추가된 사건에 대해 시점 및 상황 규칙 면에서 적절히 설계되어 있는가?
     - 초기 사건의 진단시 진단 가능한 시점인가?
     - 사건 진행 도중에 발생할 경우, 절차서 상에서 적절히(시점 및 규칙 상) 다루고 있는가?

<u>관련 계측기(운전원의 상황판단 오류를 유발시킬 수 있는 계기)의 오작동 가정</u>:

3. 특정 계측기의 오기능 시 EOC 가능성 평가
   - 특정 계측기의 오기능 가능성을 운전원의 상황판단 오류로 인한 EOC를 유발시킬 수 있는 방향으로 검토하고, 다음과 같이 다중 정보를 통한 상황판단의 회복이 가능한 지를 평가한다.
     - 다중(redundant) 및 다양한(diverse) 정보의 가용성과 유용성 확인
     - 운전원의 계측 정보 확인 습성

4. 회복 가능성의 평가
   - 가용한 시간 내에 확인할 수 있는 발전소 상태 관련 유용한 정보의 확인
   - 절차서 진행 중의 회복 가능성 조사
   - 독립 점검자(예: 안전과장의 주요안전기능 확인)를 통한 확인

한편, 대응 초기 시점에서 두 번째 사건이 유발된 경우는 초기의 사건진단 절차 수행 시점과 사건진행 중의 관련 절차서 수행 중 등 두 번의 기회를 통해서 운전원의 사건진단 또는 상황파악 가능성을 고려할 수 있다. 이 때, 두 번째 유발 사건의 발생 시점에 대한 합리적인 기준 설정이 필요하다.

- Case 3 : 주어진 초기사건과 관련된 절차서 수행 중 발생 가능한 EOC 분석.

이 경우에서는, Case 2와 같은 사건진행 도중의 유발사건이 없이, 주어진 초기사건에 적절한 대응 절차서를 이용하여 사건을 완화시키는 활동을 수행하는 도중에 발생할 수 있는 EOC 가능성을 분석한다. 이러한 EOC의 유형은 대부분 해당 발전소의 초기사건에 대한 PSA ET(Event Tree)로부터 도출 가능하다. 크게 다음과 같은 단계로 분석이 가능하다.

- 해당 초기사건에서 요구되는 시스템 기능을 파악한다.; 예) 보조급수의 공급
- 각 기능에 대하여 가능한 EOC 유형을 정의한다.; 예) 부적절한 기능 종료
- 각 EOC 유형에 대해 그러한 조치를 유발케하는 상황적 조건의 존재 가능성을 파악한다.

세 번째 단계에서 고려될 수 있는 상황적 조건에는 다음과 같은 물리적 상황 조건 및 운영적, 기술적 조건 등이 있을 수 있다. 여기에서 기술되지 않은 다른 조건들도 타당한 메

커니즘 하에 추가될 수 있다.

- 가압기 만수위 방지, RCS 과냉각 방지, 주요 펌프 보호 등 운전 관습 또는 절차서 규정 등에 의해 운전원의 주의를 요하는 물리적 상황
- 새로운 사건 유발의 징조, 발전소 운영상 복잡한 상황의 전개 예상, 과거 경험이 있는 사건의 발생 예상 등이 존재하는 상황
- 주요 계측기의 고장 및 오작동 모드와 확률
- 다중 계기에 대한 가용성 및 유용성 점검
- 주요 시스템의 자동작동 전 선(先) 조치에 대한 해당 발전소의 훈련 관습
- 주제어실 정보 시스템의 설계 문제: 혼동 가능성있는 제어기/스위치/버턴 등의 배치

4. 적 용

위의 제3절에서 제시한 분석체계에 따라 고리 3,4호기의 일반과도사건 시 분석 대상 EOC로 고려될 수 있는 EOC 사건을 도출하였다. 본 논문에서는 이들의 발생 가능성에 대한 상세 분석 결과를 제시하는 수준은 아니며, 다만 분석 결과로 제시되는 EOC 사건들이 분석 대상 EOC 사건으로 고려될 수 있음을 제시하는 수준이다. 이들에 대한 상세 분석은 상세 EOC 분석 절차가 마련되고 그에 따른 체계적인 분석을 통해 이루어져야 한다. 고리 3,4호기 일반과도사건의 사건수목이 그림 1에 제시되어 있다. 제3절에서 제시한 각 Case에 따라 분석 결과를 정리하면 다음과 같다.

- Case 1: EOP 상으로 일반과도사건과 혼동될 수 있는 초기사건은 거의 없는 것으로 가정한다.
- Case 2: 다음의 세 가지 추가적 사건이 고려된다.
  ① PORV와 PSV의 고착 개방(Stuck-open)으로 인한 SLOCA/MLOCA 발생
  ② 2차측 급수의 완전상실 (주/보조급수의 완전상실)
  ③ 주증기 안전밸브의 고착 개방으로 인한 LSSB 발생

  첫 번째 ①의 경우 PORV와 PSV의 고착 개방 경우는 조금 다르게 다룰 필요가 있는데, PORV의 고착 개방 시에는 block valve의 자동 닫힘이 back-up으로 작동하도록 설계되어 있다. 그러므로, PORV의 고착 개방에 대한 고려 시에는 block valve의 자동닫힘 실패 가능성을 고려해야 하므로 발생 확률이 상당히 낮다. 일단 고착 개방이 발생하게 되는 경우에는 이 사건의 진단 또는 상황판단 가능성 여부에 따라 TMI-2와 같은 운전원의 부적절한 조치 가능성이 고려되거나 무시할 수 있다.

  두 번째 ②의 경우인 급수완전상실 상황에서는 상황판단 오류로부터 EOC 사건의 가능성보다는 EOO, 즉 누락오류 가능성이 더 현실적이다.

  세 번째 ③의 경우에는 계기 오류 등으로 인해 운전원의 부적절한 상황모델이 형성되면 증기발생기의 고수위 지시로 인해 급수량 감소 또는 차단과 같은 EOC 조치를 취할 가능성이 있다.

- Case 3: Case 2에 해당되지 않는 시스템 기능으로부터 다음과 같은 EOC 사건들이 고려될 수 있다.

  Secondary Heat Removal:
  - MFWS/AFWS inappropriately removed from automatic control
  - MFWS/AFWS inappropriately terminated
  - MFWS/AFWS inappropriately isolated or aligned
  - Steam Dump Valves or Steam Relief Valves inappropriately isolated or aligned

  Feed and Bleed Operation:
  - PORV block valves inappropriately isolated or aligned

  HPSI Recirculation:
  - HPSI Recirculation inappropriately terminated

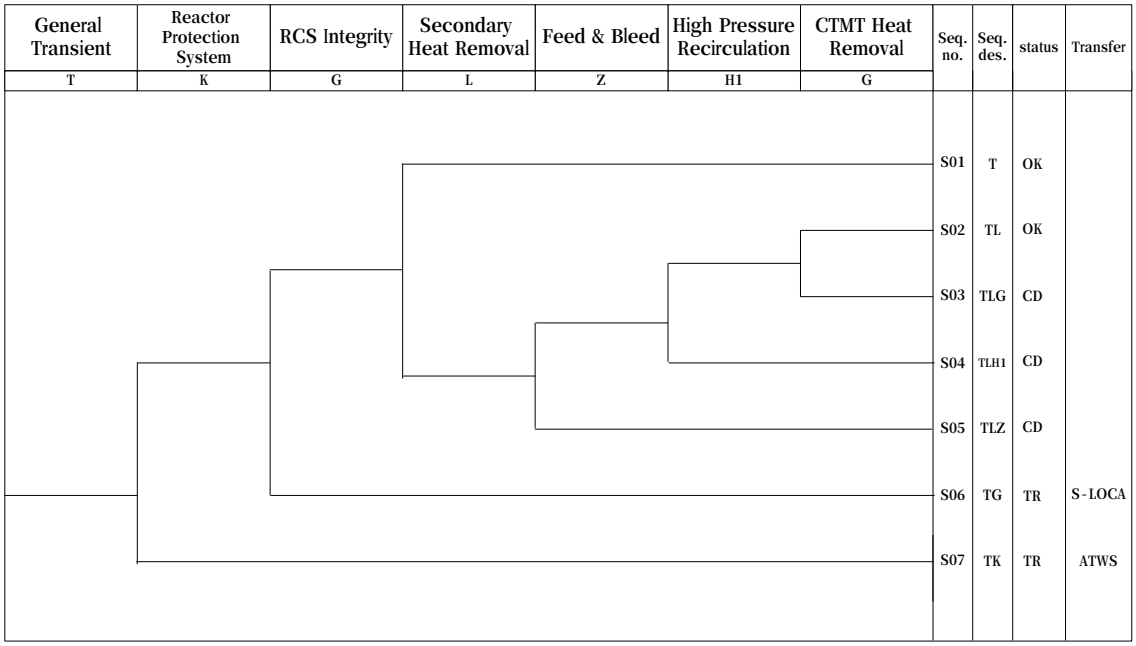

그림 1. 고리 3&4호기 일반과도 사건수목

5. 결 론

본 연구에서는 TMI-2 사고 이후 관심이 증가된 원전 운전원의 부적절한 조치(EOC: Errors of Commission) 가능성에 대한 분석의 필요성을 제시하고, 미국의 주요 원전 사건/사고에서 개입되었던 EOC 사건을 검토하고, EOC 유형과 이를 유발하게 된 상황 및 내재적 요인을 정리하였다. 또한, EOC 사건에 대한 분석 결과를 바탕으로 원전 위험도 분석 체계 내에서 EOC 사건을 분석할 수 있는 분석 체계를 제시하였고, 제안한 분석 체계에 따라 고리 3,4호기의 일반과도사건에서 고려될 수 있는 EOC 사건을 제시하였다.

본 논문에서는 원전 운전원의 EOC 사건을 도출하고 분석할 수 있는 한 분석 방향을 제시한 단계이며, 이를 바탕으로 실제 인간오류 분석자 또는 위험도 평가 업무 담당자가 사용할 수 있는 상세 분석 절차를 작성할 계획이다. 또한, 위험도 평가에서 불가피하게 고려되는 정량적 발생확률의 계산에 대한 체계도 마련되어야 할 것이다. 이와 함께, 도출된 EOC 사건의 위험도 평가 모델인 PSA에의 반영 방안도 고려하여야 할 것이다.

[감사의 글]

본 연구는 과학기술부의 원자력중장기 연구개발사업의 지원으로 수행되었습니다.

[참고 문헌]

[Dougherty, 1988] Dougherty Ed, Fragola JR, Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications, A Wiley-Interscience Publication, 1988.

[Dougherty, 1998] Dougherty Ed, Human errors of commission revisited: an evaluation of the ATHEANA approach, Reliability Engineering and System Safety, 60, 71-82, 1998.

[Meyer, 1993] Meyer OR, Hill SG, Steinke WF, Studies of human performance during operating events: 1990-1992, NUREG/CR-5953, USNRC, Washington, DC, Jan. 1993.

[Reer, 1999] Reer B, Straeter O, Dang V, Hirschberg S., A comparative evaluation of emerging methods for errors of commission based on applications to the Davis-Besse (1985) event. PSI Bericht Nr. 99-11. 1999.

[USNRC, 1985] USNRC, Loss of main and auxiliary feedwater event at the Davis-Besse plant on June 9, 1985, NUREG-1154, USNRC, Washington, DC, July 1985.

[USNRC, 2000] USNRC, Technical basis and implementation guidelines for A Technique for Human Event Analysis (ATHEANA), NUREG-1624, USNRC, Washington, DC, Rev. 1, May 2000.

[Hollnagel, 2000] Hollnagel, E., Looking for errors of omission and commission or the hunting of the snark revisited, Reliability Engineering and System Safety, 68, pp. 135-145, 2000.

[Macwan, 1994] Macwan, A., Mosleh, A., A methodology for modelling operator errors of commission in probabilistic risk assessment, Reliability Engineering and System Safety, 45(1-2), 139-157, 1994.

[Julius, 1995] Julius, J., Jorgenson, E., Parry, G.W., Mosleh, A., A procedure for the analysis of errors of commission in a PSA of a NPP at full power, Reliability Engineering and System Safety, 50, 189-201, 1995.

[Reason, 1990] Reason, J., Human Error, Cambridge University Press, 1990.

[Dang, 2001] Dang, V., Reer, B, Hirschberg, S., Analysing errors of commission: identification and a first assessment for a swiss plant, OECD/NEA Workshop on Building the New HRA: Errors of Commission – from Research to Application, Rockville, MD, May 7-9, 2001.