2004 춘계학술발표회 논문집
한국원자력학회

계측제어계통, 인간기계연계, 그리고 운전원을 통합한 시스템에 대한 정량적 안전성 평가 모형 개발

Development of a Quantative Safety Analysis Model for the Integrated System of I&C Systems, MMI, and Human Operators

김만철, 성풍현
한국과학기술원
대전광역시 유성구 구성동 373-1

요 약

확률론적안전성평가를 보다 더 현실적으로 수행하기 위해서는 인간신뢰도분석 분야의 진보가 필연적이라 할 것이다. 하지만, 현재의 인간신뢰도분석 방법들은 계측제어계통과 운전원 사이의 상호의존성에 대한 고려의 결핍, 그리고 운전원의 상황판단의 평가에 대한 이론적 기반의 부재와 같은 한계점을 포함하고 있다. 이러한 한계점들을 극복하기 위해서 계측제어계통과 인간기계연계, 그리고 운전원을 통합하는 정량적 안전성 평가 모형을 개발하였다. 이 논문을 통해서 제안되는 모형은 베이시안 네트워크를 큰 틀로 하여, 이미 개발된 RGGG 방법과 운전원의 상황판단에 대한 정량적 평가 모형을 기반으로 한다. 이 모형은 인간신뢰도분석의 현실성을 높임으로써, 확률론적안전성분석의 현실성을 보다 더 높일 수 있을 것으로 기대된다.

Abstract

To make PSA more realistic, the improvements of HRA are essential. But, current HRA methods have many limitations including the lack of considerations on the interdependency between I&C systems and human operators, and lack of theoretical basis for the situation assessment of human operators. To overcome these limitations, we develop a quantitative model for the reliability analysis of the integrated system which consists of I&C systems, MMI, and human operators. The proposed model is developed in the framework of Bayesian networks, based on the RGGG method and the quantitative model for the situation assessment of human operators. The proposed

model is expected to increase the reality of PSA, by increasing the reality of HRA in the framework of PSA

1. 서 론

원자력발전소의 운전에 있어서 안전성의 확보는 매우 중요한 문제이며, 정량적인 안전성 분석은 일반적으로 확률론적안전성평가(Probabilistic Safety Assessment, PSA)을 통해 이루어진다. 최근 위험도기반 규제 및 응용 (Risk-Informed Regulation and Application, RIRA)의 도입으로 확률론적안전성평가의 결과는 원자력발전소 운영에 중요한 자료로 사용되어지게 될 예정이다. 이는 우리가 확률론적안전성분석의 정확성을 높이는 만큼, 더 높은 안전성과 경제성을 얻을 수 있게 됨을 의미하는 것이다.

기존의 확률론적안전성평가는 매우 잘 정립되어있는 분야이나, 인간신뢰도분석(Human Reliability Analysis, HRA)의 정확성에 대한 논의는 끊이지 않고 있다. 이는 확률론적안전성평가에 있어서 인간신뢰도분석의 중요성 또는 운전원의 오류가 원자력발전소의 안전성이 미치는 영향을 고려할 때 매우 중대한 사안임을 알 수 있다. 한 연구결과는 원자력발전소의 전체 노심용융확률(Core Damage Frequency, CDF)에서 58%가 운전원의 오류에서 기인한다고 밝히고 있다.[1] 울진 3, 4호기의 확률론적안전성분석에서의 중요도 분석의 결과, 가장 높은 중요도(importance measure)를 갖는 10개의 기본사건(basic event)들 중에서 5개가 운전원 오류와 관련이 있다는 사실 또한 인간신뢰도분석의 중요성을 뒷받침한다.[2]

본 논문에서는 기존의 인간신뢰도분석 방법론에 대한 분석을 통해, 인간신뢰도분석의 정확성을 높임으로써 확률론적안전성평가의 현실성을 높일 수 있는 방안을 제안한다.

2. 본 론

2.1 사고상황 분석에 대한 이론적 배경의 필요성

사고상황에서 원자력발전소의 운전원들은 사고를 완화하기 위하여 필요한 적절한 조치들을 취해야 하는데, 이러한 조치를 취하기 위해서 가장 중요한 것은 운전원의 올바른 상황판단(situation assessment)이다. 이러한 측면에서 운전원의 올바른 상황판단 가능성에 대한 평가는 인간신뢰도분석에 있어서 가장 중요한 부분이 되어야 할 것이다. 하지만, THERP, ASEP, HCR 그리고 HEART와 같은 기존의 인간신뢰도분석 방법론은 운전원의 올바른 상황판단 가능성을 평가하는데 있어서 심지어 운전원이 처해진 상황조차도 그 고려하지 않고 있는 실정이다. 우리 나라의 확률론적안전성평가에 있어서 가장 자주 사용된 ASEP/THERP (ASEP과 THERP의 조합) 방법론의 경우, 운전원의 상황판단 오류확률은 오직 가용시간(allowable time)만을 주요한 인자(dominent factor)로 보고, 다른 인자들은

환경인자(Performance Shaping Factor, PSA)로써 부분적으로 확률을 보정하는데 이용하고 있다. [3] 또한, 가용시간에 따른 운전원의 상황판단 오류확률은 그림 1과 같이 주어지는 것으로 가정하는데, 실제 그림 1에 나타난 시간에 따른 확률의 변화는 어떠한 이론적인 배경이 있는 것이 아니라, 단순한 추정치(estimation)에 불과하다. 이러한 이유에 의해, 실제 원자력발전소에서는 운전원의 필요조치 불이행 오류(Errors Of Omission, EOO)보다는 운전원의 부적절한 조치 오류(Errors of Commission, EOC)가 원자력발전소의 안전성에 더 많은 영향을 준다는 연구 결과들에도 불구하고, 기존의 인간신뢰도분석 방법론들은 운전원의 부적절한 조치 오류에 대한 적절한 평가 방법을 제시할 수 없다는 한계점을 보이게 되었다. Hollnagel[4]이 주장한 바와 같이, 보다 발전된 인간신뢰도분석 방법들은 원자력발전소 운전원들의 행위와 그들의 수행도를 설명할 수 있는 튼튼한 운전원 모형(model)의 기반을 갖추어야 할 것이다.

2.2 계측제어계통과 운전원 사이의 상호의존성

원자력발전소의 운전원들은 자신들이 받은 훈련과 자신들이 발전소에서 쌓아온 경험들을 바탕으로 발전소에 대한 모형을 세우고, 계측제어계통에서 제공된 정보(information)들을 인간기계연계(Man-Machine Interface, MMI)를 통해서 받아들임으로써 발전소의 상황판단을 하게 된다. 따라서, 계측제어계통은 주제어실(Main Control Room, MCR)의 운전원들에게 가장 중요한 정보제공자(information provider)의 역할을 수행하게 되며, 이는 운전원의 상황판단과 계측제어계통 사이에 의존성(dependency)가 존재함을 의미하게 된다. 다른 한편으로, 계측제어계통의 일부인 발전소보호계통(Plant Protection System, PPS)이나 원자로보호안전설비계통(Engineered Safety Features Actuation System, ESFAS)에서 발생된 자동제어신호들이 운전원의 상황판단에 의해서 우회(bypass)될 수 있다는 측면에서, 이러한 신호에 대한 신뢰도와 운전원의 상황판단 사이에 의존성이 존재한다는 것이다. 다시 말해서, 계측제어계통과 운전원 사이에는 상호의존성(interdependency)가 존재한다는 것이며, 따라서 계측제어계통과 인간기계연계, 그리고 운전원은 서로 다른 개체가 아닌 하나의 통합된 개체로 보아야 함을 의미한다.

그림 2는 울진 3, 4호기 확률론전안전성평가에서의 고장수목(fault tree)의 일부분으로써, 기존의 확률론적안전성평가에서 계측제어계통과 운전원이 어떻게 모형화(modeling)되고 있는지 보여주고 있다. 그림 2에서 볼 수 있는 바와 같이, 기존의 확률론적안전성평가에서 계측제어계통과 운전원은 서로 독립적(independant)인 개체로 모형화 되어 있음을 알 수 있다. 이는 위에서 언급된 계측제어계통과 운전원 사이의 상호의존성을 고려하고 있지 않음을 의미하고 있다.

2.3 정량적 상황판단 모형의 개발

많은 종류의 상황인식(situation awareness) 모형들[5-7]이 개발되어져 있고, 그들은 대부분 상황판단(situation assessment)의 과정에 대한 설명을 포함하고 있다. 하지만, 이러한 모형들의 정성적(qualitative)이고, 묘사적(descriptive)인 특성으로 인하여 어떤 사건에 대한 회귀적(retrospective) 분석에는 매우 유용할 수는 있으나, 앞으로 일어날 일에 대한 예견적(predictive) 분석에는 한계점을 드러낼 수 밖에 없다. 하지만, 확률론적안전성평가는 앞으로 일어날 사건에 대한 예견적 분석을 위한 방법인 만큼, 확률론적안전성평가의 틀 안에서 적용되는 인간신뢰도분석 역시 예견적 분석이 가능한 정량적(quantitative) 상황인식 모형에 기반하고 있어야 할 것이다. 하지만, 아직까지는 몇몇 정량적(quantitative) 상황판단 모형만이 개발되어 있을 뿐이고, 이들 또한 많은 한계점을 가지고 있었다.

이에 따라, 저자들은 기존의 한계점들을 극복한 새로운 정량적 상황판단 모형을 개발하였다. [8] 새로이 개발된 상황판단 모형은 다음의 두 가정에 기반한다.

1. 운전원들 대략적으로 Bayes의 정리에 기반한 추론을 할 수 있는 능력이 있다. 하지만, 그 결과는 수학적 계산의 결과만큼 정확하지는 못할 것이다.
2. 운전원이 지식기반의 정보습득의 과정을 수행할 때, 운전원들은 가장 많은 정보를 주는 것으로 기대되는 지시계(indicator)의 값을 읽고자 한다.

실제 운전원들이 가지고 있는 한계점에 대한 인식을 바탕으로, 먼저 이상적인 운전원들(ideal operators)의 상황판단에 대한 수학적 모형을 Bayes의 정리와 정보이론(information theory)에 기반하여 개발하였다. 하지만, 개발된 이상적인 운전원들의 상황판단의 과정에 대한 수학적 모형과 실제 운전원들이 사고상황에서 행하는 상황판단의 과정에는 어느 정도의 일관성이 있을 것으로 추측되고 있다. 이에 따라, 새로이 개발된 이상적인 운전원들의 상황판단에 대한 수학적 모형을 기반으로, 실제 운전원들의 상황판단에 대한 실험적인 결과들을 추가한다면, 실제 운전원들의 상황판단에 대한 정량적인 모형을 개발할 수 있을 것으로 예상된다.

2.4 계측제어계통, 인간기계연계, 그리고 운전원이 통합된 시스템에 대한 정량적 모형

이미 위에서 원자력발전소에서 계측제어계통과 운전원들 사이에는 상호의존성이 존재하며, 그에 따라 계측제어계통, 인간기계연계, 그리고 운전원은 하나의 통합된 개체로 보아서 안전성 평가를 수행하여야 한다고 언급하였다. 위에서 언급한 운전원들의 상황판단에 대한 정량적 모형을 기반으로 해서, 계측제어계통, 인간기계연계, 그리고 운전원을 통합한 시스템에 대한 정량적 안전성 평가 방법을 개발하였다. 이러한 정량적 안전성 평가 방법은 베이시안 네트워크 (Bayesian network)를 기반으로 개발되었으며, 원자력발전소에서의 계측제어계통, 운전원 사이의 정보의 흐름과 다시 원자력발전소로 되돌아가는 제어신호를 기술하고 있다. 이들 중, 계측제어계통 내부에서의 정보의 흐름은 저자들에 의해 개

발된 Reliability Graph with General Gates (RGGG) 방법론[9]에 의해 표현될 수 있으며, 운전원의 상황판단은 위에서 언급한 정량적 상황판단 모형에 의해서 표현될 수 있다. 이러한 통합시스템에 대한 정량적 안전성 평가를 통해서, 확률론적안전성평가에서의 계측제어계통과 운전원에 대한 평가를 보다 더 현실적으로 수행할 수 있을 것으로 판단된다.

3. 결 론

확률론적안전성평가를 보다 더 현실적으로 수행하기 위해서는 인간신뢰도분석 분야의 진보다 필연적이라 할 것이다. 하지만, 현재의 인간신뢰도분석 방법들은 계측제어계통과 운전원 사이의 상호의존성에 대한 고려의 결핍, 혹은 운전원의 상황판단의 평가에 대한 이론적 기반의 부재와 같은 한계점을 포함하고 있다. 이러한 한계점들을 극복하기 위해서 우리는 계측제어계통과 인간기계연계, 그리고 운전원을 통합하는 정량적 안적성 평가 방법을 개발하였다. 이 논문을 통해서 제한된 방법은 베이시안 네트워크를 큰 틀로 하여, 이미 개발된 RGGG 방법과 운전원의 상황판단에 대한 정량적 평가 모형를 기반으로 개발되었다. 이 논문에서 제안된 방법은 인간신뢰도분석의 현실성을 높임으로써, 확률론적 안전성분석의 현실성을 보다 더 높일 수 있을 것으로 기대된다.

감사의 글

이 연구는 과학기술부의 국가지정연구실(National Research Lab., NRL) 사업의 지원에 의해 수행되었습니다.

참고문헌

[1] IAEA Workshop on Improvement of Safety and Economics of NPP, 2002
[2] KEPCO, Full scope level 2 PSA for Ulchin unit 3&4: Internal event analysis, 1998t
[3] A. D. Swain and H. E. Guttman, Handbook of human reliability analysis with emphasis on nuclear power plant applications, NUREG/CR-1278, U. S. Nuclear Regulatory Commission, 1983
[4] Hollnagel E. Cognitive reliability and error analysis method. Elsevier, 1998
[5] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems", Human Factors, vol.37, pp.32-64, 1995

[6] G. Bendy and D. Meister, "Theory of activity and situation awareness", International Journal of Cognitive Ergonomics, vol.3, pp.63-72, 1999
[7] M. J. Adams, Y. J. Tenney, and P. W. Pew, "Situation awareness and the cognitive management of complex sytems", Human Factors, vol.37, pp.85-104, 1995
[8] M. C. Kim and P. H. Seong, "A quantitative model for situation assessment of nuclear power plant operators based on Bayesian inference and information theory", Submitted to IEEE Transactions on Nuclear Science, 2004
[9] M. C. Kim and P. H. Seong, "Reliability graph with general gates: an intuitive and practival method for system reliability analysis", Reliability Engineering and System Safety, Vol.78, pp.239-246, 2002

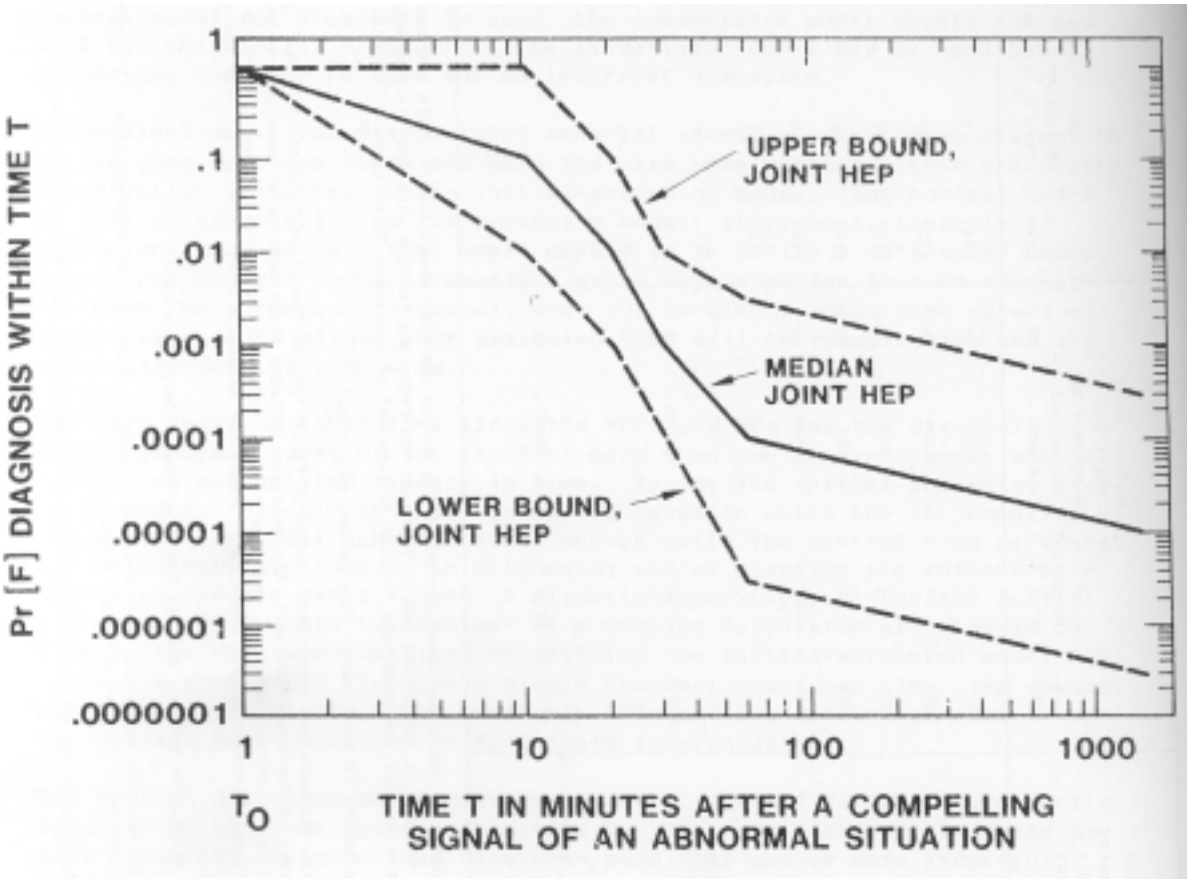

그림 1 ASEP/THERP 방법에서의 상황판단에 대한 시간에 따른 실패확률

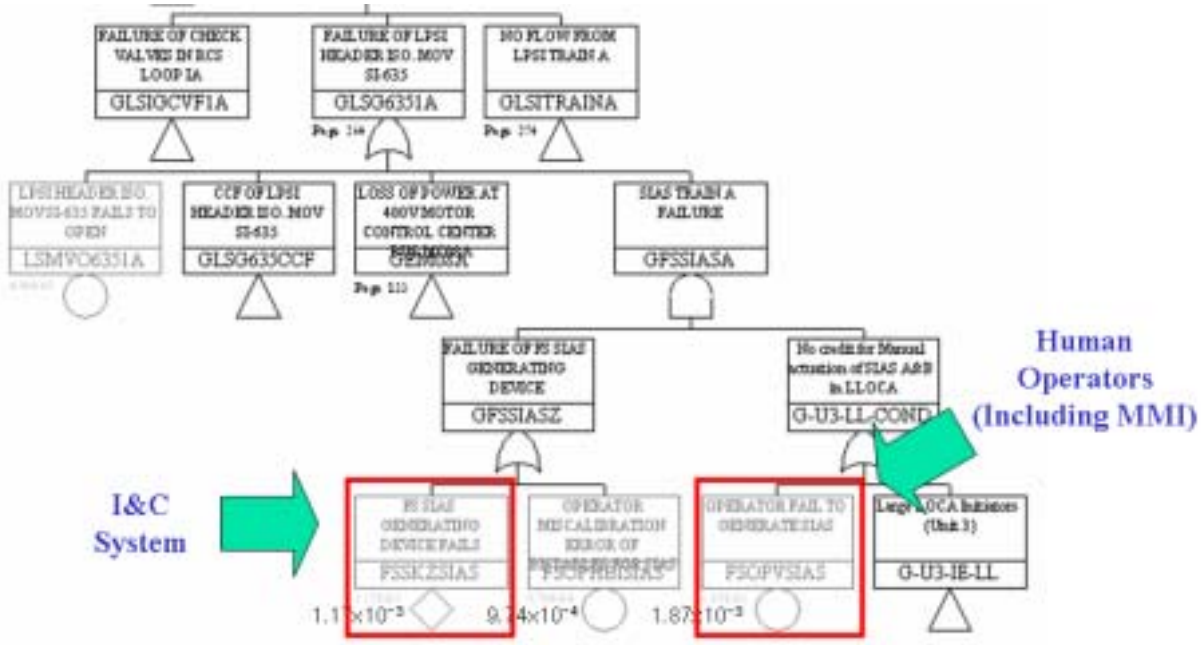

그림 2 기존의 PSA를 위한 고장수목의 일부분에서 계측제어계통과 운전원의 해당 부분