2002 춘계학술발표 논문집
한국원자력학회

디지털 안전계통의 정량적 안전성 평가를 위한 체계적 접근

A Systematic Approach for the Quantitative Safety Assessment of Digital Safety Systems

강현국, 성태용, 하재주

한국원자력연구소
대전광역시 유성구 덕진동 150

요 약

원전 안전계통에의 디지털 계통의 적용이 가시화됨에 따라 정량적 안전평가는 중요한 현안으로 부상하고 있으면서도 그동안 체계적인 접근방법이 부재하였다. 원전 안전계통 자체의 복잡성과 디지털 계통 고유의 복잡성에 기인하여 디지털 안전계통의 정량적 안전성 분석은 대단히 복잡한 분석과정을 거치게 된다. 본 논문에서는 이러한 디지털 계통의 안전성을 보다 체계적이고 구체적으로 평가하기 위한 접근방법을 제시하였다. 모두 3단계로 이루어진 이 방법론은 연구의 체계이기도 하면서 동시에 안전성 평가의 체계이기도 하다. 첫 번째 단계는 원전전체의 안전성에 디지털계통이 미치는 영향을 평가하는 것인데 이를 통해 구체적인 계통의 분석 수준을 결정하게 된다. 두 번째 단계는 디지털계통 차원의 안전성 분석인데, 다중 채널에 대한 공통원인 고장의 처리 및 상호 감시 체계의 적절한 평가가 이에 해당한다. 세 번째 단계는 계통의 안전성 분석에서 요구되는 세부 인자들의 값 추정인데, 디지털 계통의 특성상 기존의 아날로그 계통이나 기계 구조에 비해 잘 정립되어 있지 못한 부분이므로 특히 중요한 변수를 중심으로 값을 산출해야 한다. 현실적으로 모든 상황에 대해 모든 변수를 최대한의 정밀도로 고려하는 것이 불가능하므로, 본 논문에서 제시하는 방법을 통해 비용-효과 측면에서 합리적인 결과를 얻을 수 있을 것으로 기대한다.

Abstract

In recent days the number of applications of digital equipment to the safety systems of nuclear power plants are much increased. This paper proposes a systematic approach with which we could assess the safety of digital systems in a more detailed manner. This approach consists of 3 steps: The first is assessing the importance of digital systems' failure to the plant-level safety. The result of this analysis would be helpful to decide the scope of PSA and the depth of modeling. The second is modeling digital system itself whose result would show important factors that should be modeled in the PSA of digital systems. The third is estimating the values for selected important factors. Then finally we will get the reasonable result of the PSA of digital I&C systems.

제 1 장 서론

비안전계통의 경우에는 원자력 발전소에도 이미 디지털 기기들이 도입되어 활용되고 있다. 또한 최근에는 기존 아날로그 보호계통 기기들의 성능저하, 노후화, 부품 품귀 등의 이유로 인해, 극히 보수적으로 취급되어 온 안전관련 계통에서도 디지털 기기의 도입이 시도되고 있다. 국내의 경우, 중수로인 월성 원전에서는 안전정지 계통에 이미 디지털 기기들이 도입하여 활용하고 있으며, 경수로에서도 영광 3,4 호기에 마이크로프로세서를 활용한 Interposing Logic System을 도입하므로써 안전 관련 계통에의 디지털 기기의 적용이 시작되었다.

전세계적으로 연구·설계중인 차세대 원자력 발전소의 중요한 특징 중의 하나는 디지털 계측제어계통의 전면 채택이라고 할 수 있다. 디지털 계통 설계의 채택이 단순화와 표준화를 용이하게 하며 운전중 유지보수 측면에서도 많은 장점을 지닌 것으로 판단되기 때문이다. 우리나라의 울진 5,6 호기도 이러한 세계적인 추세와 같이 디지털기기를 적극 활용하고 있어 안전계통인 원자로정지계통과 공학적 안전설비 작동계통에도 디지털 기기를 적용하고 있으며 가동중인 원전에 대해서도 노후 기기에 대한 디지털 기기로의 대체가 추진되고 있다.

그러나 디지털 계통으로의 대체 필요성이 이렇게 강하게 제기되고 있고, 실제로 그 대체

가 진행중인데 비해, 디지털 계통에 대한 정량적인 신뢰도 평가 방법이 확보되어 있지 않아 그 안전성 확보에 어려움을 겪고 있다. 기존의 아날로그 기기의 경우에는 정해진 사용구간(입력 범위)내에서 연속적인 거동을 보이므로, 몇 개의 입력 샘플에 대한 결과값을 이용하여 기기의 신뢰도를 평가하는 것이 가능하다. 디지털 기기는 아날로그 기기와는 달리 그 특성이 연속적이지 않다는 점에 정량적 평가의 어려움이 있다. 즉, 디지털 기기는 한정된 샘플 시험값들 만으로는 전 사용구간에서의 성능을 추론할 수가 없다는 것이다. 따라서 현재로는 하드웨어에 대해서만 제조자가 제공한 자료를 바탕으로 고장율을 추정하고 있으며, 소프트웨어의 부분에 대해서는 엄격한 명세서와 그 이행사항을 반영한 고품질의 개발 공정을 채택했는지의 여부의 검증 및 확인을 중심으로 정성적인 평가만이 가능하며, 최종 제품의 필수 기능을 검증하는 정도의 실제 시험만이 이루어지는 것이 현실이다.

디지털 시스템에 대해서는 기존의 아날로그 시스템에 적용하던 평가 방법과는 크게 다른 방법론의 적용이 요구되고 있다. 범용 하드웨어 시스템에 소프트웨어를 통해 기능을 부여하는 방식부터 아날로그 시스템과는 크게 다르다. 아날로그 기기에서는 우발성 결함(random 결함)이 주요 결함 요인이었지만, 디지털 기기에서는 하드웨어의 우발성 결함 이외에도 소프트웨어 설계 결함으로 인한 결정론적 결함(deterministic 결함)까지도 고려해야 할 필요가 있다. 소프트웨어 설계의 결정론적 결함은 시험을 통해 완전히 제거하는 것이 불가능하다는 것이 소프트웨어 공학 연구의 대체적인 결론이기 때문이다.

또한 공통의 범용 하드웨어를 사용하고 환경에 민감한 기기의 특성상 공통원인 고장(common cause failure)에 대한 우려가 높아졌다. 소프트웨어의 경우도 코드의 공유나 데이터의 공유가 활발해지므로써 공통원인 고장의 우려를 높이고 있다. 이러한 공통원인 고장의 파급은 원자력 발전소의 안전을 위해 필수적인 다중성을 상실시킬 가능성을 높이므로 이를 방지하기 위해 다양성의 확보와 함께 기기의 고품질에 대한 보증이 요구되고 있다. 그러나 전술한 바와 같이 기기의 고품질을 보증할 수 있는 정량적 방법론이 개발되어 있지 않은 상태이므로 이러한 문제에 효과적으로 대응할 수 없다.

디지털 기술 특유의 불확실성·불명확성을 극복하고 원자력발전소의 안전관련 분야에 적용하기 위해서는, 확률론적 안전성평가(Probabilistic Safety Assessment; PSA)와 같은 정량평가 방법의 적극적인 활용이 중요한 역할을 할 것으로 판단된다. 원전의 안전성을 종합적이며 정량적으로 평가하기 위한 중요한 안전성평가 수단으로 PSA가 사용되고 있으며, 신규 원자력 발전소 건설시 인허가 사항으로 제출이 요구된다. PSA는 논리적으로 이상사건에 대한 발전소 대응을 모델하며, 이를 통해 각 사고경위의 원인 및 발생빈도를 기기의 단위까지 파악 할 수 있으며, 각 계통의 주어진 기능을 수행실패에 대해서도 원인과 각 확률 값을 구할 수 있다. 이러한 결과는 원하지 않는 사건의 발생 확률과 원인을 밝힐 수 있기 때문에 이를 이용하여 설계 검증, 정비 최적화 등에 다양하게 이용된다. 최근에는 미국을 중심으로

PSA 결과를 결정론적인 규제의 보완 수단으로 사용하고 있으며, 국내에서도 이의 채택이 적극적으로 추진되고 있다 [1],[2]. 또한 PSA는 초기 설계 단계에 적용되어 설계 검증에 이용되며 설계 개선에도 활용될 수 있다[3].

이러한 디지털 계통의 PSA 방법론 개발에 대한 시급한 필요성에 의해 본 연구가 수행되었는데, 원전의 안전관련 디지털 계통에 대한 체계적인 분석이 기존에 수행된 바 없으므로 그 체계적인 방법론을 제시하는 것이 중요하다. 본 논문에서는 3단계 걸친 디지털계통의 안전성 분석 접근 방법을 소개한다.

제 2 장 디지털 계통 안전평가의 3단계

전술한 바와 같이 디지털 계통의 정량적 안전성 분석은 기존에 체계적으로 수행된 바가 없다. 또한 신호 생성 계통은 기존의 원전 플랜트 안전성 분석에서 심도있게 고려되지 않았었다. 아날로그 계통의 경우 각각의 신호에 대해 독립적인 회로를 유지하였고 소프트웨어가 포함되지 않은 단순한 계통이었으므로, 기기의 공통원인 고장에 대한 분석이나 소프트웨어의 오류에 의한 계통 작동 불능이 심각하게 고려될 필요가 없었다. 즉, 디지털 안전계통에 대한 정량적 안전평가는 계통 자체로도 기존의 원전 PSA에서 고려된 적이 없었고, 디지털 기기의 불가용도에 대해서도 충분한 정확도로 분석된 바 없었다.

따라서 이러한 전혀 새로운 분야에 접근하기 위해서는 단계적이고 체계적인 접근 방법이 필요하게 된다. 본 논문에서는 그동안의 PSA 경험 및 디지털 계통 안전분석의 경험에 근거하여 디지털 안전계통의 안전분석 접근 체계를 제시하고자 한다. 모두 3단계로 이루어진 이 방법론은 연구의 체계이기도 하면서 동시에 안전성 평가의 체계이기도 하다. 그림 1에 이러한 접근 방법의 개념도를 도시하였다.

첫 번째 단계는 원전전체의 안전성에 디지털계통이 미치는 영향을 평가하는 것인데 이를 통해 구체적 계통의 분석의 수준을 결정하게 된다. 기존의 PSA에서도 특정 모델의 범위와 깊이는 그 모델이 전체 계통에 미치는 영향을 고려해서 정해진다. 디지털 계통의 경우에도 이러한 1단계 분석을 거쳐 2단계에서 어느 정도 수준으로 모델링해야 하는지를 결정한다. 이때, 특히 유의해야 할 점은 안전기능에 입력신호를 제공하는 디지털 기기의 종속관계를 잘 고려해야 한다는 것이다. 기존의 PSA에서는 이러한 관계를 고려하지 않고 각각의 안전기능에 각각의 기기가 설치된 것으로 가정을 하였으나, 디지털 기기로 대체됨에 따라 이러한 종속관계가 더욱 심화될 것으로 판단되므로 정량적으로 그 종속의 정도를 적절히 반영하는 것이 디지털 계통이 전체 원전에 미치는 영향을 평가하는데 중요한 역할을 한다. 상세한 설명은 제 3 장에서 다루었다.

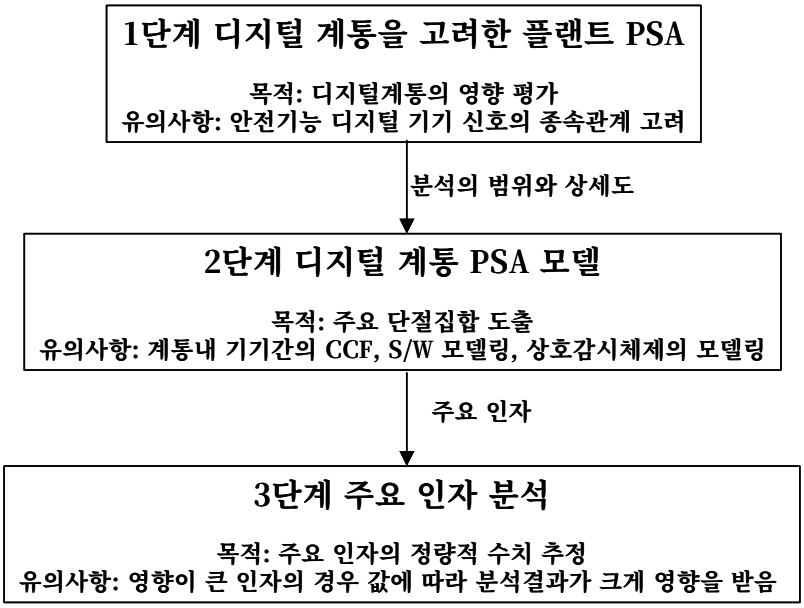

그림 1. 3단계 분석의 개념도

두 번째 단계는 디지털계통 차원의 안전성 분석인데, 다중 채널에 따른 공통원인 고장의 처리 및 상호 감시 체계의 적절한 평가가 이에 해당한다. 1단계에서 해당 계통의 중요도를 파악한 후 그 중요도에 걸맞는 분석의 범위와 깊이를 설정한 후 모델링을 수행한다. 이때 계통내의 기기 CCF(공통원인고장), 소프트웨어 오류의 모델링, 상호 감시체제 등 고장내구성 기법의 모델링에 특히 유의해야 한다. 이러한 모델링을 통해 어떠한 인자가 PSA 결과에 중요한 영향을 미치는 지를 파악할 수 있고, 그 인자들에 집중하여 정량화를 수행한다. 상세한 설명은 제 4 장에서 다루었다.

세 번째 단계는 계통의 안전성 분석에서 요구되는 세부 인자들의 값 추정을 통해 마지막 정량화를 수행하는 것인데, 디지털 계통의 특성상 기존의 아날로그 계통이나 기계 구조에 비해 잘 정립되어 있지 못한 부분이므로 특히 중요한 변수를 중심으로 값을 산출해야 한다. 기존의 연구[4],[5]에서 지적한 바와 같이 중요한 인자들의 경우 그 값을 비현실적으로 지정할 경우 PSA 결과를 수십에서 수천배까지 왜곡시킬 수 있음에 주의해야 한다. 상세한 내용은 제 5 장에서 다루었다.

제 3 장　디지털 계통의 플랜트 영향평가

1단계로 디지털 계통을 고려한 플랜트 PSA를 수행할 필요가 있다. 전술한 바와 같이 기존의 PSA에서는 각각의 안전기능에 각각의 신호 생성기기가 설치된 것으로 가정을 하였으나, 디지털 기기로 대체됨에 따라 이러한 종속관계가 더욱 심화될 것으로 판단된다. 디지털 계통은 안전 신호 생성 계통이므로, 안전성 분석을 위해서는 플랜트 PSA의 최상위 단위인 사건수목에서부터 새롭게 접근해야 한다.

사건수목은 특정한 안전기능의 작동 여부에 따라 플랜트의 사건진행상태를 나타내기 위해 사용된다. 원활한 설명을 위해 예제로서 그림 2에 대형 이차측 파단 사고에 대한 사건수목을 보였다. 먼저 그림 2의 예를 설명하자면, 먼저 초기사건인 Large secondary side break가 발생하면, RPS가 reactor를 trip시킨다. 만약 trip시키지 못한다면 이것은 ATWS에 해당하게 된다. Trip이 무사히 되었다면, 이제 기타 안전기능이 무사히 작동하느냐에 따라 플랜트의 상태가 결정되게 된다. Deliver Aux. Feedwater, HPSIS injection, HPSIS recirculation 등이 이러한 안전기능에 해당한다.

이러한 안전기능의 작동여부는 안전기능을 직접 수행하는 작동기(actuator)와 안전기능이 작동하도록 신호를 생성하는 신호생성의 건전성에 좌우된다. 신호생성은 다시 신호생성 기기의 건전성과 인간 운전원의 수동작동 적절성 여부에 좌우된다. 이것을 고장수목으로 도시하면 그림 3과 같다. 기존의 PSA에서는 그림 3에서와 같이 신호생성 기기의 고장을 하나의 기본사건으로 단순하게 처리하고 있으며, 각 안전기능들의 신호생성 기기간의 종속성은 전혀 고려하지 않고 있다.

이제 한국형 표준원전(KSNP)의 디지털화의 경우와 같이, RPS와 ESFAS를 디지털화하는 경우를 생각해 보자. 그림 2의 안전기능들 중에서 Deliver Aux. Feedwater, HPSIS injection, HPSIS recirculation은 모두 공학적 안전설비 작동계통(ESFAS)에서 생성되는 신호이며, 원자로정지(Reactor trip) 신호를 생성하는 RPS도 ESFAS와 일부 신호를 공유하고 있다. 따라서 외형적으로는 각기 다른 신호들이지만, 내부적으로는 같은 'signal generating system'에 의해 생성되는 신호인 것이다. 따라서 이러한 종속성이 적절히 반영된 사건수목 분석을 수행하고 민감도 분석 등을 수행할 경우, 디지털 기기가 안전성에 미치는 영향을 보다 합리적으로 파악할 수 있다.

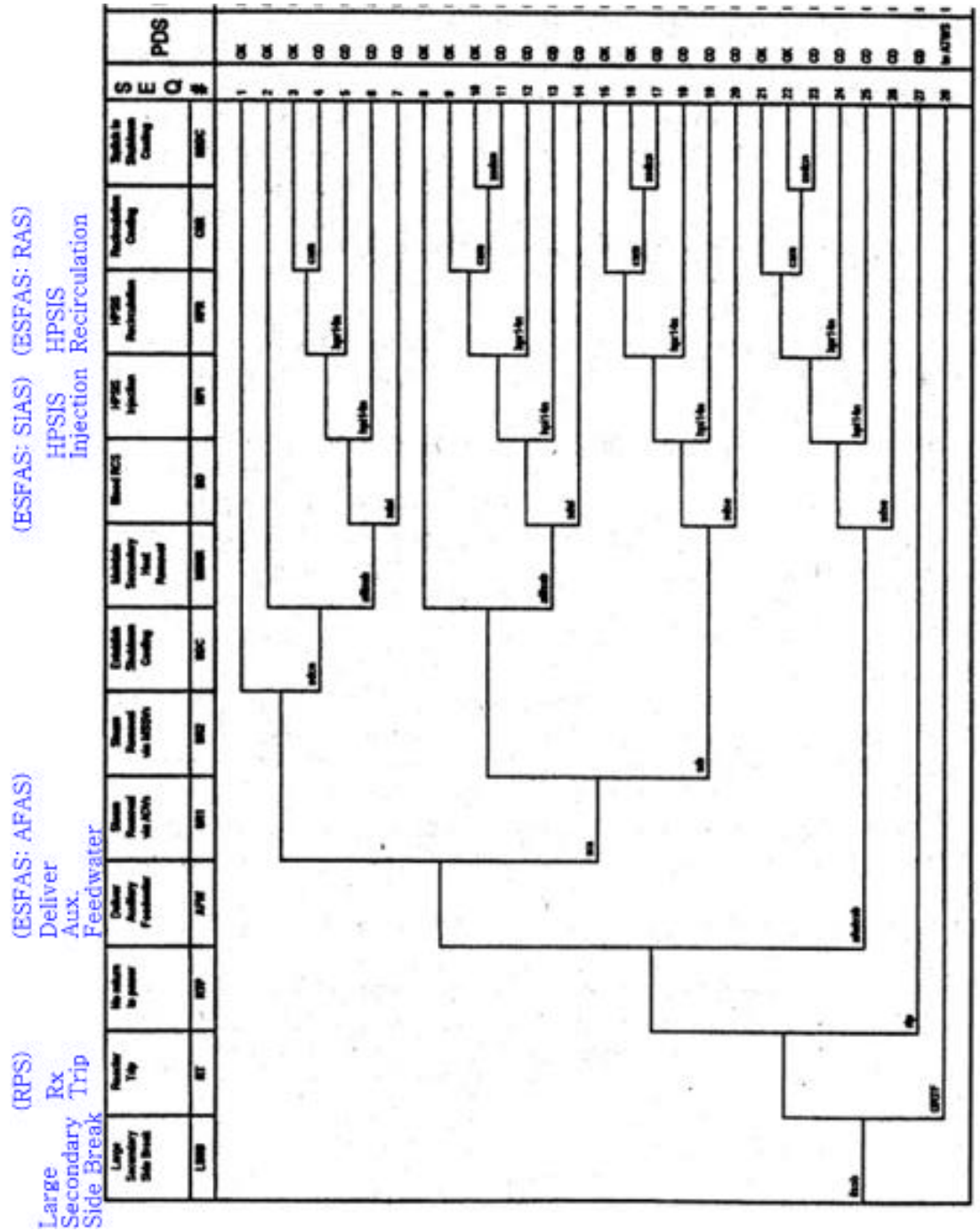

그림 2. 대형 이차측 파단 사건수목

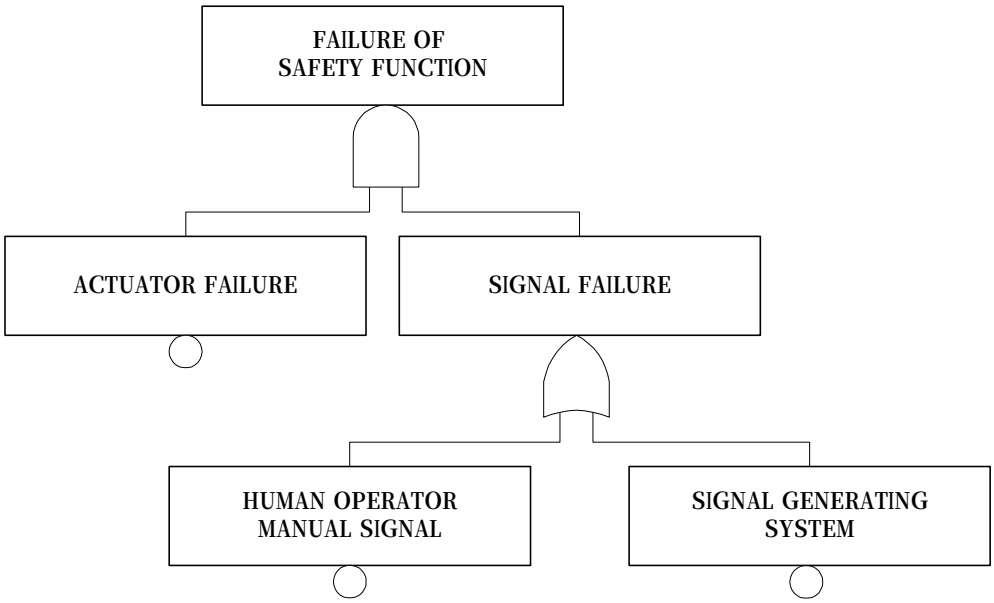

그림 3. 안전기능의 작동확률 계산을 위한 고장수목

제 4 장 디지털 계통의 모델링

2단계로는 디지털 계통 자체를 모델링한다. 이것은 고장수목을 이용한다. 전술한 바와 같이 이 단계에서는 다중 채널의 적용에 따른 공통원인 고장의 처리 및 상호 감시 체계의 적절한 평가가 매우 중요하게 작용한다. 즉, 1단계에서 파악한 해당 계통의 중요도에 걸맞는 정도의 모델을 작성하는 것이다. PSA을 위해서 모든 계통을 최대한의 깊이로 모델링을 한다면 최상의 결과를 얻을 수 있겠지만, 이것은 시간과 비용면에서 현실적이지 못하다. 따라서 기존의 PSA에서도 전체 원전의 안전성에 기준 이하의 영향을 미치는 경우는 screen out을 하고 있다. 전체 원전에 미치는 영향에 적절한 정도의 모델링 범위와 깊이를 설정하는 것은 비용-효과면에서 중요한 역할을 한다.

제 3 장에서 예시한 디지털 안전계통중에서 원자로 보호계통(RPS)을 고장수목으로 모델링하는 과정과 그 결과를 알아보자. 다중성을 갖춘 보호계통을 대상으로 하였으며, 그 모델링과 분석 결과에 대한 세부 사항은 [6]에 상세히 기술되어 있다.

고장수목을 이용한 분석의 결과는 다음과 같이 확률들의 곱으로 이루어진 단절집합들의 합의 형태로 나타나게 된다.

System Unavailability = q1+q2+ ... + qi + ... +qn

qi= p1*p2*...*pj*...*pm

이때 pj는 기본사건 j의 발생 확률을 나타내며, qi는 단절집합 i의 확률을 나타낸다. 단절집합이란 해당 기본사건들이 동시에 발생할 경우 계통의 기능 실패를 유발하는 기본사건들의 집합을 말한다.

일반적으로 다중성을 갖춘 보호계통의 단절집합들은 다음의 4가지로 분류해 볼 수 있다.

- 1 그룹: 입력신호를 전달받지 못하게 되는 경우
- 2 그룹: 정확한 출력신호를 생성하지 못하게 되는 경우
- 3 그룹: 신호의 처리를 정확하게 하지 못하는 경우
- 4 그룹: 상기의 사건들이 복합적으로 작용하는 경우

상기의 각각의 단절집합들은 개념적으로 그림 4에 도시한 바와 같이 파악할 수 있다. 1 그룹의 단절집합의 발생확률은 입력모듈 공통원인 고장의 확률이 가장 중요하게 작용할 것이며, 2, 3 그룹의 단절집합의 경우에도 결국은 출력모듈 및 프로세서 모듈의 공통원인 고장의 영향을 가장 심각하게 받을 것이다. 디지털 계통의 각 모듈의 고장확률이 10E-3/demand 이하인 점을 고려할 때, 4 그룹의 발생확률은 1, 2, 3 그룹의 발생확률에 비해 무시할 수 있을 것임이 자명하다. 예를 들어 4개의 다중성을 가진 계통을 가정해 보면, 각각의 사건들이 복합적으로 일어나는 경우는 10E-12/demand 수준의 발생 확률을 가지는데 비해 공통원인 고장은 10E-5/demand 수준의 발생확률을 가지기 때문에 공통원인 고장의 발생확률이 개별 기기의 독립고장이 복합적으로 작용할 확률보다 천만배 정도로 높기 때문이다.

따라서 주요 단절집합을 나열해 보면 다음과 같다.

q1 = Pr(OP) * Pr(AI CCF)

q2 = Pr(OP) * Pr(DO CCF)

q3 = Pr(OP) * Pr(PM CCF) * Pr(WDT CCF)

q4 = Pr(OP) * Pr(PM CCF) * { Pr(WDT a1) * Pr(WDT a3)... }

q5 = Pr(OP) * Pr(PM CCF) * { Pr(WDT a1) * Pr(DO a3)... }

이때, 각 확률은 다음과 같이 정의된다.

Pr(OP)	the probability that a human operator will fail to manually initiate the reactor trip
Pr(AI CCF)	the probability of the CCF of analog input modules
Pr(DO CCF)	the probability of the CCF of digital output modules
Pr(PM CCF)	the probability of the CCF of processor modules
Pr(WDT CCF)	the probability of the CCF of watchdog timers
Pr(WDT a)	the probability that the watchdog timer a will fail to initiate the reactor trip
Pr(DO b)	the probability that the digital output module b will fail to

initiate the reactor trip.

q1은 1 그룹에 해당하는데, 입력모듈의 공통원인 고장이 발생하여 원자로정지 계통이 정상적으로 신호를 처리하지 못하는 가운데, 운전원 또한 원자로 정지신호를 발생시키는데 실패할 확률을 나타내며, q2는 2 그룹에 해당하고, q3, q4, q5는 모두 3 그룹에 해당한다. 일반적으로 디지털 프로세서 모듈의 고장확률이 입출력 모듈의 고장확률에 비해 현저히 높지만, 감시타이머를 설치하여 프로세서 모듈의 고장을 감시하는 경우에는 감시타이머 또한 적절한 감시를 수행하지 못하는 경우에만 계통의 실패가 발생하게 된다.

상기의 주요 단절집합의 살펴보면, 운전원의 오류 확률은 디지털 계통과는 직접 관계가 없으며, q4 및 q5와 같이 개별 사건의 확률의 곱이 포함된 경우는 상대적으로 그 발생확률이 낮으므로, 주요 사건을 Pr(AI CCF), Pr(DO CCF), Pr(PM CCF), Pr(WDT CCF)의 4가지로 정의할 수 있다.

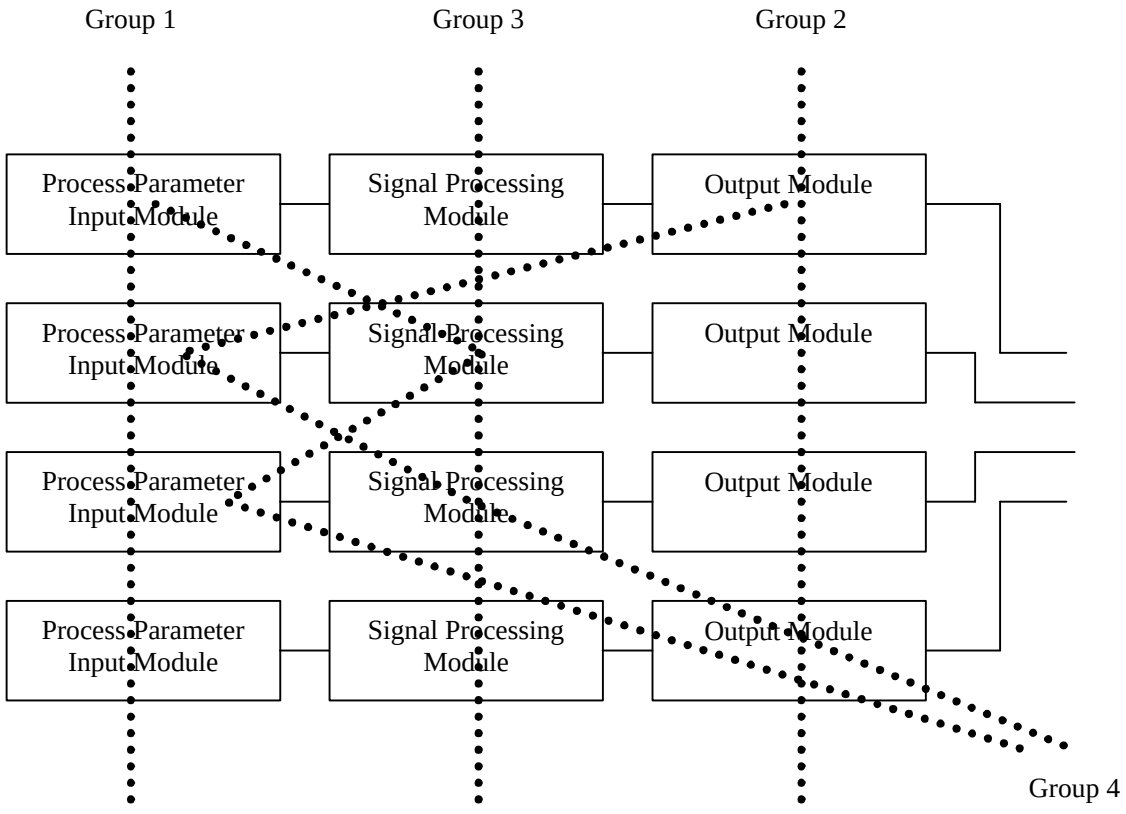

그림 4. 다중성을 갖춘 원자로 보호계통의 단절집합의 분류 개념도

제 5 장 주요인자 정량화

세 번째 단계는 계통의 안전성 분석에서 요구되는 세부 인자들의 값 추정을 통해 마지막 정량화를 수행하는 것이다. 계통의 정량화에 필요한 인자 및 변수들은 그 숫자가 너무 많으므로 비용-효과의 측면을 고려해서 2단계의 과정을 거쳐 영향력이 큰 인자만 가려내어 그 정량적 값을 추정하는 것이다.

디지털 계통은 원전에서의 사용이력이 짧아 그 고장자료가 충분하지 못하고, 특유의 비선형성으로 인해 고장 유형의 분석도 어렵다. 그러므로 하나하나의 인자를 정량화하는데 상당한 노력이 필요하며, 만약 중요 인자의 값을 잘못 추정하게되면 PSA 결과를 완전히 왜곡하게 될 수 있으므로 특히 유의해야 한다 [5].

설명의 편의를 위해 제 3 장과 제 4 장에서 제시한 예제를 통해 설명을 계속해 보자. Pr(AI CCF), Pr(DO CCF)은 입출력 모듈의 공통원인 고장 확률을 뜻하는데, 입출력 모듈의 공통원인 고장은 설계에 따라 크게 달라진다. 즉, 입출력 모듈에 모두 동종의 모듈을 사용하는지, 이기종의 모듈을 배치하여 공통원인 고장 배제 설계를 하는지에 따라 그 발생확률이 변하는 것이다. Pr(PM CCF)은 프로세서 모듈의 하드웨어적인 고장확률과 소프트웨어의 오류 확률을 나타낸다. 하드웨어의 고장확률은 어느 정도의 수준에서 크게 변화하기 어려우므로, 소프트웨어의 오류확률이 주요 인자가 된다고 하겠다. Pr(WDT CCF)은 감시타이머가 하드웨어적으로 고장날 확률과 프로세서 모듈의 고장을 감지해 내지 못할 확률을 나타낸다. 감시타이머는 매우 단순한 하드웨어 contact로 구성되어 있으므로 Pr(WDT CCF)은 주로 프로세서 모듈의 고장을 감지하지 못할 확률에 의해 영향을 받는다. 따라서 이 감지확률이 주요 인자가 된다.

위의 결과를 정리하자면, 공통원인 고장의 적용과 소프트웨어 오류확률 추정, 그리고 감시타이머의 고장감지율이 주요한 인자가 되는 것이다. 물론 각 기기 하드웨어의 기본적인 고장율 자료도 중요한 정량화 요인이 되지만, 이것은 기기 제작자가 MIL-HDBK 217 등의 자료를 통해 충분히 파악할 수 있으며 그 변화의 폭이 좁으므로 본 논문에서는 설명하지 않는다. 하드웨어 고장율의 정량적 추정에 관해서는 [7]에 상세히 설명되어 있다.

공통원인 고장(CCF)의 적용은 계통의 설계에 의해 결정된다. 디지털 안전 계통에서는 많은 수의 다중화를 기본으로 한다. 즉, 하나 또는 두개의 시스템에 의지할 경우 원전이 이상상태가 되었을 때 시스템이 제대로 구동되지 않을 가능성이 있으므로, 여러 채널에 여러 개의 시스템을 병렬로 두어 그 신뢰도를 높이는 것이다. 실제로 한국형 표준 원전의 디지털 원자로 보호 계통에서는 꼭 같은 역할을 하는 동시논리 프로세서 모듈과 디지털 출력 모듈이 각각 16개나 사용되고 있다. 그런데, 이렇게 많은 다중성을 두었다고 할 지라도 그 많은

기기가 동시에 같은 원인으로 고장을 일으키는 확률이 높다면 그 다중성은 효력을 상실하게 된다. 이처럼 디지털 시스템의 경우 위험도가 일부 기기에 집중되게 되므로 특히 CCF의 처리가 중요하다. CCF의 처리 방법에 따라 PSA결과가 크게 달라지기 때문이다. 서로 상이한 제작자의 제품이라 할 지라도 동일 부품을 이용하거나 동일 소프트웨어를 이용함으로써 CCF의 확률을 가질 수 있으므로 세심한 처리가 필요하다.

소프트웨어 오류의 모델링과 관련하여, 실제 적용에 있어서는 그 발생의 무작위성을 인정하는 '고장률'을 이용하는 경우가 많은데, 이것은 소프트웨어에 대한 고장률 개념은 '빈도'가 아니라 '기대치(확신도)'의 개념이기 때문이다. 테스트 결과 한번도 오류를 일으킨 적이 없는 소프트웨어가 잠재되어 있던 문제점으로 인해 '앞으로의 실제 사용시 고장을 일으킬 것으로 기대하는 정도'를 추정하는 문제가 되기 때문이다. 하드웨어의 경우에는 각 부품들의 고장률에 관한 많은 표준을 참고할 수 있으나 소프트웨어는 이 같은 것이 없으므로 직접적인 테스트가 필요하게 된다. 원자력발전소의 안전계통에 오류가 발견된 소프트웨어를 그대로 적용하는 것을 상정하는 것은 비현실적이다. 따라서 테스트를 몇회 수행하던지 간에, 소프트웨어 관련하여 발생한 오류가 없는 결과를 얻게 될 것이다. 위에 언급한 바와 같이 '앞으로의 실제 사용시 고장을 일으킬 것으로 기대하는 정도'를 추정하기 위한 기본 자료로 테스트 횟수를 사용하는 것이다. 테스트 방법 개발의 핵심 요소는 테스트 횟수의 결정, 하드웨어 고장과 소프트웨어 고장의 구분, 테스트 입력자료 생성, 테스트의 coverage 산출로 정리될 수 있다.

원전에 적용되는 디지털 계통의 경우, 외부에 별도의 감시 타이머를 장착하여 계통을 감시하는 방법을 많이 이용한다. 감시 타이머는 디지털 시스템에 이상이 생겼을 경우, 이를 감지해 내기 위한 가장 기초적인 장치인데, PLC와 같이 주기적인 반복실행(cyclic operation)을 위주로 하는 시스템에 특히 효과적으로 적용될 수 있다. 감시 타이머는 하드웨어 interrupt를 발생시키는 일종의 interval timer로서, 일정시간 이상 신호가 발생하지 않을 경우 시스템에 문제가 생긴 것으로 판단하여 원자로 정지 신호를 발생시킨다. 이것은 "정해진 시간을 초과하는 코드 실행은 시스템의 오류를 의미한다"는 가정하에 이루어진다. 그러나 모든 시스템의 오류가 시간지연을 유발하는 것은 아니므로, 감시 타이머의 유효범위는 제한되어 있다는 점에 유의하여야 한다. 문제는 이와 같은 유효 검출 범위를 추정하는 것이 쉽지 않다는 것이며, 감시 타이머만을 이용한 경우에 그 검출 범위의 상한은 0.6-0.7 정도임은 선행연구를 통해 밝혀져 있다 [8].

제 6 장 결론 및 논의점

기존의 아날로그 기기는 더 이상 원전에 사용할 수 있는 정도의 고신뢰도 부품이 생산되지 않기 때문에 불가피하게 디지털 기기로 대체될 수밖에 없는데, 우리나라는 추후 원전을 지속적으로 건설할 계획이므로 계속적인 디지털 기기의 안전계통 적용이 이루어질 전망이다. 이러한 산업 상황에서 디지털 기기에 대한 안전평가 기법의 발달은 원전에 대한 새로운 기기와 알고리듬 적용을 활성화하여 궁극적으로 국내 원자력산업계의 경쟁력확보에 큰 도움이 될 것이다.

그러나 실제로는 디지털 기기의 안전평가에 관한 기술이 정립되어 있지 않아, 새로운 설계의 적용이나 기존 설계의 변경에 많은 장애가 되고 있다. 원전 안전계통 자체의 복잡성과 디지털 계통 고유의 복잡성에 기인하여 디지털 안전계통의 정량적 안전성 분석은 대단히 복잡한 분석과정을 거치게 되는데, 본 논문에서는 이러한 디지털 계통의 안전성을 보다 체계적이고 구체적으로 평가하기 위한 접근방법을 제시하였다. 모든 상황에 대해 모든 변수를 최대한의 정밀도로 고려하는 것은 현실적으로 불가능하므로, 본 논문에 제시된 방법을 통해 비용-효과 측면에서 합리적인 결과를 얻을 수 있을 것으로 기대한다.

이러한 연구를 통해 현재 국내에서 진행중인 많은 원전 계측제어 기기 개발 과제에 바탕을 제공할 수 있을 것으로 생각하며, 개발 연구와 안전성 평가 연구가 협력 발전할 경우 우리나라가 이 분야의 선진 기술을 확보할 수 있는 계기가 될 것으로 기대한다. 세계 원전 주도국들을 중심으로 이루어지고 있는 제4세대 원전 개발에는 신개념의 디지털 계측제어 기법의 활용이 증대되어 이에 대한 위험도 평가 기술개발은 더욱 활발히 이루어질 전망이므로 이 분야 대한 기술 수요가 계속 발생할 것으로 판단되므로 더욱 집중적인 연구가 필요할 것으로 생각된다.

참고문헌

[1] U.S. NRC, Options For Risk-Informed Revisions to 10 CFR Part 50 - "Domestic Licensing of Production And Utilization Facilities" SECY-98-300, 1998.

[2] 이창주, 안전규제에서의 위험도 정보 활용 원칙, KINS/AR-306, Vol 5. Part I, 원자력안전기술 정보회의, 1999.

[3] 성태용 외, 확률론적 안전성 평가기법을 이용한 보조급수계통의 설계 최적화 연구, '92 한국원자력학회 춘계학술발표회, 1992.

[4] 강현국 외, 확률론적 안전성 평가에서의 디지털 계측제어 계통 고유현안 분석, KAERI/AR-560/2000, 2000.

[5] Hyun Gook Kang and Taeyong Sung, "A Quantitative Study on Important Factors

of the PSA of Safety-Critical Digital Systems," Journal of Korea Nuclear Society, Vol. 33, No. 6, 2001.

[6] Hyun Gook Kang and Taeyong Sung, "A design guide of digital I&C systems from the viewpoint of PSA," Proceedings of 2001 conference of CUP's nuclear I&C subtask, Nov. 8-9, Cheju, Korea, 2001.

[7] 정환성 외, "디지털 계측제어기기의 하드웨어 신뢰도 정량 평가 방법 비교 연구", KAERI/TR-2119/2002, 2002

[8] A. Mahmood and E.J. McCluskey, "Concurrent Error Detection Using Watchdog Processors: A Survey," IEEE Trans. On Computers, Vol. 37, No. 2, February 1988.