'96 춘계 학술발표회 논문집
한국원자력학회

원자로 보호계통의 공통원인고장시 사고해석 방법론에 대한 고찰

권영민*, 송진호, 박종균
한국원자력연구소

요 약

최근에 개량형 또는 수동형 발전소의 디지탈 보호계통에서 소프트웨어의 역할이 증가함에 따라 공통원인고장의 가능성이 중요한 관심사항이 되었다. 아날로그 보호계통에서는 공통원인고장 가능성이 없었으며, 비록 공통원인고장이 발생하더라도 부식과 조기마모와 같은 과정은 천천히 진행되므로 이제까지 큰 문제가 되지 않았다. 이러한 아날로그 설계의 특징은 컴퓨터를 이용한 소프트웨어를 포함하고 있는 디지탈계통에는 적용되지 않는다. 본 논문에서는 소프트웨어의 공통원인고장을 고려하여 원자로 보호계통의 적합성을 다양성 및 심층방어 측면에서 해석할 수 있는 방법론에 대하여 논의한다. 본 논문의 결과는 추후에 한국형 차세대 원자로(KNGR)의 계측제어계통 설계를 위하여 수행하여야 할 다양성 및 심층방어 해석의 방법론 정립에 도움이 될 것으로 예상된다.

1. 서 론

원자력발전소에서 디지탈 계측제어기술의 활용은 과거에는 비안전계통의 보조계통에서 부분적으로 활용되었으나 최근에는 개량형 및 수동형 발전소인 AP600, SBWR, System 80+의 계측제어계통에서 100% 디지탈 계통을 채택하고 있으며, 한국형 차세대 원자로(KNGR)에서도 이를 적극 활용할 예정이다. 발전소 계측제어계통은 감시, 조절 및 발전소 필수기기와 공정기기들을 보호함으로써 발전소가 안전하게 운전되도록 도와준다. 디지탈 계측제어계통은 기존에 운전되는 발전소보다 훨씬 많은 data base(소프트웨어)나 공정기기(하드웨어)를 공유하고 마이크로프로세서나 컴퓨터를 기본으로 사용하는 계통이다. 이런 계통에서 하드웨어의 설계오류 및 프로그래밍 오류를 포함한 소프트웨어의 설계오류는 해당 기기의 고장 뿐 아니라 관련된 여러 기기의 고장을 야기시킨다. 특히 프로그램을 작성하는 소프트웨어 설계자의 인간적인 오류는 동일한 소프트웨어를 사용하는 모든 모듈에 잠재할 가능성이 있다. 컴퓨터나 프로세서 등은 대부분 유사한 구조를 가지고 있으므로 비록 기능이 다르더라도 동일한 프로세서를 쓰거나 동일한 시스템 소프트웨어를 쓰게 되면 공통원인고장이 여러 기능의 동시고장으로 나타날 수 있다.

다양성과 심층방어 해석은 대상계통이 공통원인고장에 대하여 적절한 다양성과 심층방어 개념을 유지하면서 설계되어 있음을 보여주기 위하여 사용하며, 또한 공통원인고장의 취약성에 대처하기 위한 설계요건을 수립하는데 사용한다. 본 논문에서는 원자로 보호계통의 공통원인고장시 다양성 및 심층방어 해석 측면에서 사고해석을 수행하는 방법론에 대하여 고찰한다.

2. 공통원인고장에 대한 다양성 및 심층방어 해석의 역사적 배경

NRC Staff은 1978년 웨스팅하우스의 혁신적 설계인 RESAR-414[1]의 통합보호계통(Integrated Protection System : IPS)의 심층방어 설계를 검토하기 위하여, 1979년에 발간된 NUREG-0493 [2]에서 공통원인고장과 관련된 다양성 및 심층방어 해석방법을 처음으로 소개하였다. NUREG-0493은 비록 웨스팅하우스 설계에 적용된 특별한 경우였으나 공통원인고장과 관련된 일반적인 법칙들이 잘 확립되어 있어서 NRC는 이를 근간으로 하여 GE의 ABWR, SBWR, 웨스팅하우스의 AP-600 설계를 검토하였으며, ABB-CE는 이들 법칙을 System 80+의 계측제어계통인 NUPLEX 80+의 심층방어해석에 사용하였다.

NRC Staff은 SECY-91-292 [3]에서 디지탈 컴퓨터 기술을 사용하는 계측제어계통의 공통원인고장 가능성을 기술하면서 품질과 다양성을 공통원인고장에 대처하는 두 가지 주요한 요소로 택하였다. 즉, 높은 품질을 유지함으로써 각 부품 및 전체계통의 신뢰도를 증가시킬 수 있으며, 하드웨어 및 소프트웨어, 운전원 조작과 같은 기능들에 대하여 다양성을 갖춤으로써 공통원인고장이 전파될 수 있는 확률을 감소시킬 수 있다. 또한 신뢰도가 높은 아날로그 백업(backup) 계통으로 다양성의 수준을 높이도록 요구하였다.

EPRI는 소프트웨어의 신뢰도를 정확하게 정량화할 수 있는 허용기준이 없음을 염두에 두었기 때문에 EPRI ALWR 설계요건서[4]의 인간-기계 연계계통(Man-Machine Interface System)에서 계통수준의 안전기능을 수행할 수 있는 백업용 수동작동 능력을 계측제어계통에 포함시킬 것을 고려하였으며 또한 계측제어계통의 심층방어 설계를 강조하였다.

NRC Staff은 디지탈 계측제어계통 설계에서 적절한 다양성을 확보하기 위한 잠정적인 규제지침을 1992년 6월에 초안하여 ACRS, 산업체, 원자로 공급자들의 검토를 거쳤다. NRC Staff은 처음에 제안한 SECY-91-292를 변경하여 다양성과 심층방어를 확보하기 위한 4가지요건(Four- point requirement)을 SECY-93-087[5]에서 처음으로 언급하였다가 1993년 7월 SRM(Staff Required Memomorandum)에서 4가지요건을 다음처럼 수정하여 공포하였다 : ① 계측제어계통의 공통원인고장의 취약성이 적절하게 보완되었는지 다양성과 심층방어 측면에서 평가되어야 한다. ② 안전분석보고서(SAR)의 사고해석에서 평가되는 각 사고에 대하여 공통원인고장을 가정할 때, 이에 대응하는 다양성이 설계에 적절히 반영되어 있음을 보여주어야 한다. ③ 만약 공통원인고장이 안전기능의 수행을 불가능하게 하면 같은 기능을 수행하거나 다른 기능을 수행하는 다양한 수단이 제공되어야 한다. ④ 운전원이 안전기능을 지원하는 변수들을 감시하고 주요 안전기능을 계통수준의 수동조작으로 작동시킬 수 있도록 안전등급의 표시장비와 제어기들이 주제어실에 설치되어야 한다.

1994년에 계측제어계통의 공통원인고장과 관련된 NRC의 기술적 관점을 반영한 NUREG/CR-6303 [6]이 발간되었다. NUREG/CR-6303은 원자로 보호계통 공통원인고장시 다양성 및 심층방어해석을 수행하는 방법론을 기술하고 있다. 이 보고서에서는 원자로 보호계통에서 발생 가능한 공수행시 요구되는 가정 및 해석절차가 포함되어 있다.

2. 공통원인고장의 대처방안

2.1 원자로 보호계통에서 독립성과 다양성

적절한 다중성이 설계에 고려되었음에도 불구하고 무작위적이 아닌 다중고장이 발생하는 경우, 이런 유형의 고장을 공통원인고장이라고 한다. 공통원인고장은 기능적이고 환경적인 영향뿐 아니라 인간행동에 기인한 사건을 포함하는 인과관계에 의해 다중고장이 유발되는 것을 포함한다. 물리적이고 전기적으로 독립성을 가지도록 설계하는 것은 공통원인고장 대처방안의 시작일 뿐 마지막은 아니다. 예를 들어서 원자로 정지계통의 한 채널의 신호가 제어계통의 입력신호로 동시에 사용되는 경우, 제어계통과 정지계통 양쪽 모두의 계측 고장은 제어계통을 통하여 과도 상태를 유발시킬 것이며, 이러한 경우 안전한 정지를 위해 필요한 원자로 정지계통의 기능은 상실될 것이다.

독립성(independence)은 서로 다른 방어체계에서 단순히 분리된(seperated) 계측채널을 사용하는 것만으로는 확보되지 않는다. 현재의 계측기술 수준에서 필요한 독립성을 제공할 수 있는 방법은 다음 두 가지이다. 첫째, 계통의 설계, 설치 및 운전시 물리적이고 전기적이며 기능적인 독립성을 유지하도록 충분한 주의를 기울이며, 둘째 적절한 다양성(diversity)을 제공하는 방법이다. 양쪽 방법 모두 필요하며 동시에 적절한 수준으로 적용되어야 한다. 첫번째 방법은 안전관련 계측계통에 대한 기준, 표준 및 규제지침들로 이미 이와 관련된 많은 사항이 잘 정립되어 있다. 두번째 방법은 본 논문의 주제로 방어계층간의 다양성은 필수적이며 심층방어 해석의 주된 관심이다. 다양성은 공통원인고장의 결과로 인해서 기능고장이 발생할 가능성을 줄이기 위한 심층방어 설계방법이다. 독립성이 연계되지 않은 다양성은 고려될 수 없다. 즉, 독립적이지 않은 요소들로 구성된 다양한 보호계통들은

상호 종속되기 때문에 동시에 고장이 발생할 수 있다. 그러므로 다양성은 규제요건이나 표준지침에서 요구되는 독립성을 대체하기 위한 수단으로 간주될 수 없으며 독립성을 대신할 수도 없다. 차라리 다양성은 예측 불가능한 공통원인고장에 대하여 계통의 강인성(robustness)을 증가시키는 독립성에 필수불가결한 요소로 보아야 한다.

2.2 심층방어 설계

심층방어 개념은 원자력발전소의 안전조치 및 설비에 대한 종합적인 전략으로서 기본적인 방법은 물리적인 방어벽을 차례로 설치함으로써 기기의 고장 또는 사람의 실수로 인한 방사성 물질의 방출을 일련의 방벽을 통하여 차례로 저지 또는 지연시켜 공중의 안전을 보존한다. 방어계층(Echelon of Defense)은 원자로 계측제어계통에 심층방어 원칙을 적용시킨 것으로서 제어계층, 원자로 정지계층, 공학적 안전설비 작동계층과 감시 및 지시계층의 순서로 이루어져 있으며 각 기능을 수행하는 계통의 이름으로 불리워지기도 한다. 제어계통이 고장나면 원자로 정지계통이 반응도를 감소시키고, 제어계통과 원자로 정지계통이 동시에 고장날 경우에는 공학적 안전설비 작동계통이 작동하여 핵연료를 냉각시킴으로써 방사성 물질이 방출되는 것을 막는 물리적 방벽을 보호한다. 그리하여 운전원이 하여금 반응도를 감소시키기 위한 다른 수단을 강구할 수 있는 여유시간을 확보시켜 준다.

서로 다른 방어계층에서 동시고장은 무작위적으로 또는 인과관계에 의하여 발생할 수 있으나. 공통원인고장과 관련된 심층방어 해석에서는 인과관계에 의하여 하나 이상의 방어계층에 고장이 일어나는 경우가 관심의 대상이다. 인과관계에 의한 고장은 소프트웨어 및 하드웨어의 부적절한 설계, 열악한 환경(화재 또는 홍수), 운전원의 오작동, 유지보수상 실수나 전력원 같은 고장에 의해 야기된 다른 계통의 고장 등과 같이 여러 요인에 의하여 발생할 수 있다. 공통원인고장은 아직까지 일어나지 않았거나 생각해 보지 않았었던 유형의 사고일 수 있다. 확인될 수 있는 공통원인고장 사건들에 대해서는 계측제어 계통의 설치 및 운전시 물리적, 전기적 그리고 기능적인 측면에서 세심한 주의를 기울이는 것과 같은 일반 공학적 방법을 사용할 수 있다. 그러나 알려지지 않은 공통원인고장에 대하여 해석을 하거나 또는 그에 대응하는 다양성의 추구가 얼마나 적절한 보호기능을 제공하는가에 대한 판단은 불가능하다. 유일한 지침은 직관과 경험으로써 어떤 유형의 고장과 실수가 일어날 수 있으며 그리고 어떤 유형의 다양성이 이에 도움이 될 것인가를 예측하는 일이다.

2.3 심층방어 설계의 평가

NRC Staff은 공통원인고장에 대처하는 심층방어 설계의 평가를 위하여 다음 두 가지 방안을 고려하였다. 첫번째 방안은 하드웨어 또는 소프트웨어에서 발생 가능한 모든 가상적인 공통원인고장을 고려하여 해석을 통하여 그 영향을 가능한 상세히 평가하는 방안이고, 두번째 방안은 계통의 독립성 측면에서 허용가능한 수준을 규정한 후, 이 수준을 설계에서 만족시킴으로써 간접적으로 심층방어 설계를 평가하는 방안이다.

공통원인고장의 상세한 평가방안의 기본 생각은 계통내의 여러 지점에서 소프트웨어와 하드웨어의 공통원인고장을 가정한 후 이와 관련된 사고해석을 수행함으로써 그 영향을 상세히 평가하는 것이다. 이 해석방안은 비록 매우 지능적인 방법이지만, NRC Staff은 1979년의 당시 기술수준을 고려하여 참고문서 2에서 이 방안의 사용을 강요하지 않았다. 왜냐하면 당시에는 원자력산업계 및 NRC Staff 모두 원자로 안전관점에서 디지탈 계통에 대한 설계 및 운전의 경험이 부족했기 때문에 설계자가 가정해야 할 공통원인고장을 규정하는데 어려움이 많았다.

규정된수준의 계통독립성을 확보하는 방안은 NRC가 RESAR-414 설계를 검토할 때 사용한 방안으로서 구체적인 공통원인고장을 가정하여 상세평가를 수행하는 대신에 계통분리성의 허용수준(acceptable degree of system separation)을 규정하여 심층방어 평가의 지침으로 삼았다. RESAR-414[1] IPS의 계측기기들의 방어계층은 가상적인 공통원인고장 사건들이 허용범위를 벗어나는 결과를 초래하지 않도록 충분히 분리되고 다양성을 갖추어 설계되도록 요구되었다. NRC가 요구한 분리와 다양성이 IPS의 심층방어 설계에 충분히 반영되었다고 판단하였기 때문에 자세한 가상사고와 개별적인 공통원인고장에 대한 상세해석이 필요하지 않았다.

3. 심층방어 해석지침

다양성 및 심층방어 해석의 수행시 필요한 일반지침이 참고문서 6에 자세히 설명되어 있다. 본 절에서는 전체적인 심층방어 해석과정에서 이들 지침이 어떻게 이용되는가에 대하여 간략하게 기술한다. 먼저 원자로 보호계통의 구성기기와 모듈을 취급 가능한 작은 기능별 단위인 블럭으로 구성한다. 이때 블럭은 소프트웨어 오류를 포함하여 모든 내부고장이 일어날 수 있는 기기와 소프트웨어의 물리적인 집합이며 한 블럭에서의 고장은 다른 블럭으로 전파되지 않는 경계조건을 만족시킨다. 전형적인 블럭의 보기로 컴퓨터, LAN, 멀티플렉서와 PLC 등을 들 수 있다. 해석대상 계통을 블럭으로 구성한 후, 해석목적과 연관된 블럭들 중 동일한 블럭으로 취급될 수 있는 블럭들과 다양성으로 고려될 수 있는 블럭들을 조사하여 심층방어 측면에서 방어계층을 구분한다. 각 블럭은 "black box"로 취급되므로 블럭 내에서 발생된 고장은 그 블럭에서 출력되는 모든 신호를 훼손시키므로 하류의 블럭들에 고장이 전파된다고 가정한다. 고장난 블럭의 출력신호들은 해석에 가장 나쁜 결과를 초래하는 방향으로 가정된다. 고장의 전파모드는 물리적(예 : 전기적)인 경우와 논리적(예 : 손상된 데이타 또는 소프트웨어 설계고장으로 인한 손상된 상호영향)인 경우로 나누어 질 수 있다. 앞서 언급된 지침들에 의하여 원자로 보호계통에서의 공통원인고장의 가능 경로를 상세히 조사한 후, 안전분석보고서(SAR)의 15장에 제시되어 있는 모든 사고에 대하여 공통원인고장을 함께 가정하여 사고해석을 수행한다.

설계기준 예상운전과도상태가 공통원인고장과 함께 발생하는 경우, 실제적인 가정과 최적 계산 방법론을 사용하여 계산된 해석결과 누출방사선량이 10 CFR 100 방사선량 제한치의 소량(10%) 이상 초과하지 말아야 하며 일차 냉각재 압력경계의 건전성을 손상시키지 않아야 한다. 설계기준 사고(accident)가 공통원인고장과 함께 발생하는 경우, 발전소 누출방사선량이 10 CFR 100 방사선량 제한치를 초과하지 말아야 하며 일차 냉각재 압력경계와 격납건물의 건전성을 손상시키지 않아야 한다. 심층방어 해석은 앞서 언급된 목표를 달성하기에 충분한 다양성이 존재함을 보여주고 또한 발견된 취약점과 그를 보완하는 적절한 조치를 명시하여야 한다.

4. System 80+ 설계의 심층방어 해석

4.1 NUPLEX 80+의 심층방어 설계

System 80+의 계측제어계통인 NUPLEX 80+ 안전관련 표시기기는 DIAS-N (Discrete Indication and Alarm System-N Channel), DIAS-P(P 채널) 및 DPS(Data Processing System)의 3부분으로 구성되어 있다. DIAS-N 기기는 보호계통 소프트웨어의 공통원인고장의 영향을 받을 수 있으므로 이 계통에서 발생되는 경보 및 표시들은 심층방어 설계를 평가하는 해석에서 유용하지 못하다고 보수적으로 가정한다. 필수안전기능과 관련된 주요 변수들은 DIAS-P를 통하여 표시되며 이들 표시기기는 참고문헌 4에서 제시된 네가지요건을 준수한 것이다. DIAS-P는 RG 1.97 [7]에서 지정한 카테고리 1의 안전변수들을 표시하는 전담기기들로서 감지된 신호가 하드웨어적으로 곧장 표시기에 표시되므로 보호계통 소프트웨어의 공통원인고장에 영향을 받지 않고 제 기능을 수행할 수 있다. DPS는 DIAS-N이 제공하는 지시 및 경보들을 다양성과 다중성 측면에서 추가적으로 제공하는 비안전등급의 계통으로서 보호계통의 공통원인고장의 영향을 받지 않는다. DPS는 Process-Component Control System(P-CCS), Power Control System(PCS)과 Engineered Safety Feature-CCS (ESF-CCS)로부터 표시 및 경보에 대한 정보를 받는다. P-CCS와 PCS는 비안전등급인 제어계통의 일부이므로 가상의 보호계통 공통원인고장의 영향을 받지 않는다. ESF-CCS를 통하여 DPS에 전달되는 정보는 가상의 보호계통 공통원인고장 영향을 받으므로 이와 관련된 정보는 심층방어 해석에서는 유용하지 않다고 가정한다. 그러나 공학적 안전설비 기기중 운전원의 수동조작으로 작동 가능한 일부 기능은 공통원인고장 상황에서도 사용 가능하다. DPS는 이들 정보들의 신호가 타당한지 자체 검증한 후, 이들 신호를 DIAS-N에 의해 검증된 신호와 비교하여 두 계통에서 검증된 신호가

서로 불일치할 때 경보를 발생한다. 운전원은 DPS와 DIAS-N에서 표시되는 해당변수들을 DIAS-P 표시기기의 변수와 비교함으로써 어떤 계통에서 비정상적인 주요 변수들이 발생되는지 알 수 있게 된다. NUPLEX 80+는 필수기능과 성공경로를 포함하는 발전소 상태변수들을 실시간으로 표시하는 대형화면 표시기인 IPSO (Integrated Plant Status Overview)가 주제어실에 설치되어 있어 주제어실 어디에서라도 발전소 상태를 감시할 수 있다. IPSO에서 표시되는 필수기능의 상태와 주요 발전소 변수들은 DPS에 의하여 지원을 받으므로 공통원인고장의 영향을 받지 않는다.

4.2 NUPLEX 80+의 다양성 및 심층방어 해석

ABB-CE는 여러가지 공통원인고장 상황에서 이에 대처하는 다양한 기기의 능력을 평가하기 위하여 bounding analysis 방법을 택하였다. 즉, 보호계통 소프트웨어를 사용하는 모든 자동운전과 이들 계통을 이용하여 작동하는 수동운전이 불가능하다고 가정하여 심층방어 해석을 수행하였다. ABB-CE의 초기 NUPLEX 80+ 심층방어 해석[8]은 기존의 15장 해석결과와 NUPLEX 80+에서 제공하는 다양성 및 심층방어 설계를 고려하여 정성적으로 평가되었다. NRC Staff은 ABB-CE가 수행한 초기의 다양성 및 심층방어 해석을 검토한 결과 SAR 15장에 기술되어 있는 28가지 사건 중 19가지에 대해서는 공통원인고장에 대응하여 적절한 보호동작을 수행하는 다양한 기기들의 능력이 입증되었다고 결론지었다. 그러나 나머지 9가지 사건들에 대하여서는 NRC의 4가지요건[4]을 적용하고 공통원인고장의 영향을 받지 않는 운전원의 수동조치를 고려하여 재평가할 것을 요구하였다. ABB-CE는 9가지 사건에 대하여 CESSAR-DC에서 재해석을 수행함으로써 다양한 기기들의 능력과 합당한 운전원 동작이 공통원인고장에 대한 적절한 보호대책이 될수 있음을 제시하였다. 재해석시 노심냉각유지, 일차냉각재계통 및 격납건물의 과압 방지, 과도한 소외선량 방출방지와 운전원 대응시간의 기준은 기존의 SAR 15장 사건 발생확률에 보호계통 소프트웨어의 공통원인고장과 같은 낮은 확률의 사건이 동시에 발생한다는 점을 고려하여 설계기준초과사고(beyond DBA)의 범주에서 결정하였다.

보호계통 소프트웨어의 공통원인고장을 가정한 사고가 발생했을 때, 즉각적인 복구운전을 수행하거나 그 영향을 단기적으로 완화시키기 위해서는 운전원의 개입이 필수적이다. 수동운전을 위한 운전원 조치시간은 비상운전지침서(EPGs)에 제시된 각 사건별 절차를 검토하여 평가되었다. 각 단계에서 요구되는 시간은 ANS/ANSI-58.8 Standard [9] 및 그 부록의 개정판 초안과 Accident Prevention Group의 보고서인 참고문서 10을 기준으로 하였다. 원자로 정지가 요구될 때 발생되는 경보지시기와 운전원에게 익숙한 다른 지시기들의 가용성 및 참고문헌 10의 실험적인 대응시간에 대한 자료들을 고려해 볼 때, 초과설계기준사고에서 운전원은 원자로 정지경보 발생 후 2분 내에 수동으로 원자로 정지운전을 시작할 수 있다고 평가된다. 그러나 실제 사고해석에서는 30분에 운전원이 수동으로 원자로를 정지시킨다고 보수적으로 가정하였다.

NUPLEX 80+의 심층방어 설계에 대하여 상세해석이 수행된 9가지 사고 해석에서는 정상적인 초기운전 조건을 사용하고, 소외전원 상실사고를 제외한 경우에는 원자로 냉각재펌프가 계속 운전가능하며, 주증기 및 급수계통과 NSSS 제어계통은 공통원인고장의 영향을 받지 않는 것으로 가정하였다. 또한 대체보호계통(APS)은 가압기 고압력 신호에 의하여 원자로를 자동정지시키고, 대체비상급수작동계통(AEFAS)은 증기발생기 저수위 신호에 의하여 비상급수를 자동공급한다고 가정하였다.

직경 12인치 이상의 배관이 파단되는 냉각재 상실사고의 경우는, 파단 부위가 대형으로 발전되기 이전에 계측기로 누출을 검출할 수 있으므로 운전원이 그 동안에 원자로 정지 및 발전소 계통을 감압시킬 수 있다. 따라서 직경 12인치 이하의 배관이 파단되는 소형냉각재 상실사고에 대해서만 보호계통 소프트웨어의 공통원인고장을 가정한 다양성 및 심층방어 해석을 수행하였다. 배관의 직경이 12인치 이상일지라도 유효 파손면적이 12인치 직경의 배관 면적보다 작은 경우는 해석에 고려하였다. CESSAR-DC에서는 6인치 가압기 안전밸브, 3인치 저온관 노즐파손과 원자로 상부의 CEA 이탈에 해당하는 $0.041ft^2$ 파손 소형냉각재 상실사고에 대해서 보호계통의 공통원인고장 가정을 고려한 해석을 수행하였다. 사고기간 중 원자로 냉각재 펌프는 운전원이 수동으로 정지시키기 전까지 운전

되는 것으로 가정하였다. 노심의 냉각가능성 기준은 10 CFR 50.46 기준을 사용하였다. 0.041ft^2 소형 냉각재 파단사고는 소외선량 관점에서도 평가되었다.

증기관 파단사고의 경우는 격납건물 외부에서 주증기관이 양단으로 파단되는 사고가 해석되었다. 증기관 파단은 노심의 과출력, 노심의 냉각가능성, 소외선량과 첨두 일차냉각재계통 압력측면에서 그 영향을 평가하였다. 증기관과 급수관을 격리시키고 가용한 다양한 기기를 이용하여서 안전주입수 작동을 수행하는데 필요한 운전원 조치시간은 30분으로 가정하였다. 증기발생기 수위는 자동조절되므로 증기발생기에서 방출되는 증기량과 동일한 급수량이 공급되다가 정상적인 급수재고량이 상실된 이후에는 공기추출 저장탱크와 응축수 저장탱크의 물이 급수되지만 사고발생 후 10분 내에 이들 역시 고갈된다. 증기발생기 수위가 저수위 설정치에 도달하면 보조급수가 공급된다. 비냉각재 상실사고에 대하여 냉각가능성 기준은 10 CFR 50.46에 제시되어 있는 핵연료봉 피복재 온도가 2200 °F로 유지되는 것이다. 비록 DNBR이 냉각가능성 기준으로 사용되지는 않지만, 일단 DNBR이 허용 핵연료설계제한치(SAFDL)인 1.24이상으로 유지되면 피복재 온도가 2200 °F 한계를 넘지 않는다고 볼 수 있으므로 CESSAR-DC 해석에서는 DNBR이 냉각가능성 기준으로 대신 사용되었다.

급수관 파단사고의 경우는 격납건물 내에서 급수관이 양단으로 파단된다고 가정하였다. 격납건물 외부의 급수관이 파단되는 경우는 격납건물 내부의 체크밸브가 증기발생기로부터의 급수 방출을 멈추게 한다. 따라서 격납건물 내부에서 체크밸브 하류에 위치하는 급수관의 파단이 격납건물 압력에 미치는 영향을 평가하였다. 이때 증기관 및 급수관의 자동폐쇄는 공통원인고장의 영향을 받지 않으므로 주급수는 급수원이 고갈되기까지 증기발생기 수위제어를 위하여 계속 공급된다. 이 사고의 허용기준은 ASME Service Level C Stress limit에 해당하는 격납건물 내부 압력으로 약 145 psia에 해당된다. 첨두 일차냉각재계통 압력 및 소외선량 측면에서의 영향은 공통원인고장을 가정한 주증기관 파단사고보다 덜 심각하므로 평가되지 않았다.

증기발생기세관 파단사고와 유출관(letdown line) 파단사고는 일차계통이 느리게 감압되는 사고이므로 제어계통의 역할이 보다 효과적이다. 이들 사고의 경우 핵연료 훼손을 방지하는 최소 운전원 조치시간을 30분으로하여 해석을 수행하였다. 유출관 파단사고의 경우 파단으로 인한 일차냉각재계통 압력감소는 가압기 압력 제어계통의 운전에 의하여 전열기가 작동되어 적절하게 보상되지만 가압기 수위는 계속 감소된다. 계통의 감압률은 공통원인고장을 가정한 증기발생기세관 파단사고보다 작으므로 DNBR 측면에서의 영향은 덜 심각하다. 외부선량 측면에서는 기존의 SAR 15.6.2절에서도 30분내에 자동으로 원자로 정지가 발생하지 않으므로 보수적인 초기조건을 사용한 SAR 15.6.2절보다 그 영향이 덜 심각하다. 증기발생기세관 파단사고의 경우는 30분 후에 수동으로 증기발생기가 격리된다. 따라서 핵연료봉 파손으로 인하여 오염된 냉각재가 세관을 통하여 방출되어도 응축기를 거쳐 air ejector에서 제거되므로 사고초기에 증기발생기를 격리를 가정하는 기존의 SAR 15.6.3.1 해석에 비하여 소외선량 측면에서 덜 심각하다. 증기발생기 수위는 자동제어되므로 증기발생기 충만(overfilling)은 발생하지 않는다.

냉각재유량 완전상실사고, 단일 원자로 냉각재펌프 회전자의 고착 및 펌프축의 파손사고의 경우는 135% 과출력 여유도를 고려하여 평가하였다. 이들 사고의 경우는 계산된 최소 DNBR이 SAFDL 이상으로 유지되어야 한다. 소외전원상실로 인하여 사고가 시작되는 냉각재유량 완전상실사고의 경우는 운전원의 조치가 없어도 사고발생 후 약 4초 후에는 CEA 구동기구의 전원공급선인 4.16KV 모선에 전원이 상실되므로 제어봉이 노심으로 자동으로 낙하되어 원자로는 정지된다. 노심의 열은 초기에는 자연순환에 의하여 증기발생기를 통해서 제거되다가, 증기발생기 수위가 대체비상급수작동계통(AEFAS)이 작동되는 저수위 설정치에 도달하면 비상급수와 주증기 안전밸브를 통하여 열제거를 수행한다. 단일 원자로 냉각재펌프 회전자 고착 및 펌프축 파손사고의 경우 건전한 3대의 원자로 냉각재펌프는 외부전원으로 전력을 공급받으므로 노심유량은 사고 후 2초 내에 초기유량의 75%로 감소되어 그 상태로 계속 유지된다.

원자로 제어봉 집합체 이탈사고의 경우는 DNBR외에도 노심의 냉각가능성 및 핵연료 엔탈피 측

면에서 평가되었다. 일차계통의 파손이 수반되는 집합체 이탈사고의 경우는 10 CFR 50.46의 기준과 소외선량 관점에서 평가되었다. 일차계통 파손이 수반되지 않는 제어봉 집합체 이탈사고의 경우는 사고발생 후 100ms 내에 노심출력이 최대 출력까지 증가한 후 그 후 서서히 100% 출력으로 감소한 후 원자로 정지가 되지 않으므로 100% 출력 상태에서 유지된다. 첨두 일차냉각재계통 압력은 사고 초기 수초 내에 발생한 후 공통원인고장의 영향을 받지 않는 가압기 압력제어계통의 살수 영향으로 감압된다. DNBR 계산은 135% 과출력 여유도를 고려하여 평가하였다.

5. 결론

NUREG/CR-6303은 계측제어계통 전체에 대하여 하드웨어 및 소프트웨어 측면에서 상호연계 되어 있는 모든 설계를 상세히 검토하여 공통원인고장이 가능한 모든 경우를 조사한 후, SAR 15장의 각 사건에 대하여 그 영향을 평가한다. 반면에 CESSAR-DC에서는 계측제어계통의 개별적인 공통원인고장 가능성을 조사하지 않고 임의의 보호계통 소프트웨어의 공통원인고장에 의하여 모든 보호계통 및 ESF작동계통의 자동운전과 고장난 보호계통의 데이타를 이용하는 수동운전이 불가능하다고 가정하는 bounding approach를 취한 후, SAR 15장의 각 사건을 정성적 또는 정량적으로 해석한다. 이때 제어계통, 보호계통 및 ESF작동계통간에 계통수준의 독립성과 다양성은 우선적으로 검토되어야 한다. 해석절차 면에서 볼 때, CESSAR-DC의 해석방법이 NUREG/CR-6303의 방법보다 수행하기 쉽고 간단하다. 그러나 다양성 및 심층방어 해석의 목표는 앞에서 기술한데로 두 방법 모두 동일하다.

NUREG/CR-6303의 해석방법은 공통원인고장에 취약한 부분의 설계를 구체적으로 찾아내어 관련 부분의 설계를 개선하거나 그에 대한 대처방안을 수립하는데 유용하게 쓸 수 있다. 반면에, CESSAR-DC의 bounding approach는 보호계통의 공통원인고장에 대처하는 적절한 다양성과 심층방어가 계측제어계통의 설계에 확보되어 있음을 비교적 단순한 방법으로 보여줄 수 있다는 장점이 있다. 그러나 CESSAR-DC의 방법을 따를 경우, 사고해석 결과가 허용기준을 만족함을 보임으로써 발전소 전체적인 측면에서 안전성을 규제기관에 입증할 수는 있지만, 각 계통내 또는 상호연계된 계통에서 공통원인고장의 상세한 해석이 수행되지 않기 때문에 이들 계통의 신뢰도를 확보할 수는 없다. 따라서 CESSAR-DC의 해석방법은 공통원인고장으로 인한 각 계통의 고장확률을 감소시키지 못하므로 발전소 이용율 또는 계통의 보수 및 관리 관점에서 볼 때 큰 이득을 주지 못한다. 특히 한국형 차세대원자로의 계측제어계통이 System 80+의 NUPLEX 80+를 많은 부분에서 변경한다면 NUREG/CR-6303 방법을 따라 설계단계에서부터 공통원인고장에 취약한 부분을 찾아내어 적절한 계측기 또는 제어기를 첨가함으로써 다양한 보호계획을 수립할 필요가 있다.

참고문서

1. Westinghouse Electric Corporation, "Reference Safety Analysis Report (RESAR)," Amendment 16 to SESAR-41, 1978.
2. NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," NRC, March 1979.
3. SECY-91-292, "Digital Computer Systems for Advanced Light Water Reactors," NRC, Sept 16, 1991.
4. EPRI URD
5. SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor(ALWR) Designs," NRC, April 2, 1993.
6. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," Lawrence Livermore National Laboratory, December 1994.
7. NRC Regulatory Guide 1.97,Rev.3, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accidents," NRC, May 1983.
8. IC-92-121, "Summary Results for NUPLEX 80+ Defense-in-Depth Analysis," A.W. Hyde and T.M Starr, June 19, 1992.
9. ANS/ANSI-58.8-1992, draft dated November 5, 1992, "American National Standard Time Response Design Criteria for Safety-Related Operator Actions."
10. Accident Prevention Group Report #12, Rev. 2, "Interim Report, Application of the EPRI Operator Reliability Experiments Data to Update the ANS-58.8 Standard," December 1990.