'98 춘계학술발표회 논문집
한국원자력학회

컴퓨터-기반 계측제어계통의 다양성 및 심층방어 평가

김복렬, 정윤형, 고정수, 정충회, 오성헌
한국원자력안전기술원
대전광역시 유성구 구성동 19

요 약

최근 원자력산업계 동향은 기기의 노후화, 예비품 확보의 어려움, 그리고 기존 설비에 대한 보수비용 증가 등의 이유로 아날로그 계측제어 설비들을 컴퓨터-기반 설비로의 부분적인 개선이나 전체적인 교체가 추진되고 있다. 그러나 컴퓨터-기반 설비는 소프트웨어와 하드웨어가 환경영향에 민감하고, 공통모드고장을 일으킬 수 있는 프로그래밍 설계오류의 잠재성이 있는 것으로 알려져 있다. 공통모드고장을 방지할 수 있는 가장 설득력 있는 해결방안은 철저한 품질보증, 심층방어 및 다양성 설계기법으로 평가되고 있다. 본 논문에서는 컴퓨터-기반 계측제어계통의 심층방어 및 다양성에 관한 규제기준과 정성적 평가를 위한 블록개념을 소개하고, 평가의 사례로서 CE System 80+와 국내 가동중인 W형 원전의 설비개선에서 주급수 상실시 컴퓨터-기반 설비의 공통모드고장에 따른 다양성과 심층방어계층을 평가하였다. 특히 국내 가동중인 W형 원전에 대해서는 그 평가결과를 근거로 하여 ATWS 완화설비의 설치를 제안하였다.

1. 서 론

컴퓨터-기반 계측제어계통의 다양성은 철저한 품질공정에 따라 개발된 하드웨어와 소프트웨어일지라도 공통모드고장 가능성이 충분히 있을 것으로 인식되고 있기 때문에 반드시 지켜져야 할 설계원칙이다. 다양성 설계를 실현하기 위한 효과적인 방법은 공통모드고장이 한 개 이상의 기능들을 동시에 상실시키지 않도록 선정된 기능들 간에 여러 가지 형태의 기능적 다양성을 고려하는 것이다. 기능적 다양성 개념은 NRC가 1978년에 웨스팅하우스(W) RESAR-414 설계, "컴퓨터기술을 이용한 통합형 보호계통(IPS)"의 검토에 대비한 연구결과로 발간한 NUREG-0493[1]에서 제시되었다. 이 보고서는 블록개념을 도입하였고, 공통모드고장 현안과 평가방법들을 설명하였으며, 예상운전사건과 방어계층들 간의 다양성 평가에 보수적인 분석방법을 적용하였다. 특히, 동 개념이 GE ABWR, W AP-600, 그리고 GE SBWR 원자로 보호계통의 다양성을 분석하는데 적용되었고, CE System 80+ 원자로 보호계통의 분석에도 채택되었다[2].

본 논문에서는 컴퓨터-기반 계측제어계통의 심층방어 및 다양성 규제기준과 정석적 평가를 위한 블록개념을 소개하고, 평가의 사례로서 CE System 80+와 국내 가동 중인 W형 원전의 설비개선에서 주급수 상실시 컴퓨터-기반 설비의 공통모드고장에 따른 다양성과 심층방어계층을 평가하였으며, 국내 가동중인 W형 원전에 대해서는 ATWS 완화설비의 설치를 제안하였다.

2. 심층방어 및 다양성에 관한 규제기준 및 블록개념

NRC는 신형로 원자로 보호계통의 다양성 평가에 NUREG-0493을 적용하여 얻은 검토경험을 바탕으로 개량형 원전의 컴퓨터시스템에 관한 주요 안전현안을 다루는 SECY-91-292[3]을 발행하였고, SECY-93-087[4]를 통해 4가지 다양성 및 심층방어에 관한 규제요건들을 제시하였다. 또한 NRC는 검토경험의 반영, 분석기법의 일부 보완, 특정사항의 삭제, 그리고 원자력위원회의 기술적 입장 등을 고려하여 NUREG/CR-6303을 발간하였으며, 이와 같은 일련의 검토 및 연구 활동들을 종합하여 심층방어 및 다양성 평가기준을 NUREG-0800 (개정 4, 1997), BTP-19[5]를 통해 발간하였다. 이 평가기준은 Reg. Guide 1.70과 NUREG-0800, 15장의 소외 피폭방사선량기준을 참조한 것이다.

NUREG-0493 또는 -6303은 원자로 보호계통의 기능적 다양성과 심층방어 계층들을 체계적으로 분석하기 위해 블록개념을 도입하였다. 블록개념은 계통의 기기 또는 모듈을 다루기 쉬운 작은 기능블록들로 분해하는 것을 의미한다. 즉 임의의 계통설계에 대한 심층방어분석을 수행하려면 먼저 그 계통의 구성요소들을 정의하고 기능적으로 유사한 구성요소들을 한데 모아 놓는 것을 블록(block)이라고 하며, 이것이 심층방어분석에 필요한 하나의 기본단위가 된다. 컴퓨터-기반 계측제어계통에 대한 다양성 및 심층방어분석을 수행하기 위한 대표적인 방식은 센서와 신호처리 부분들을 그림 1과 같이 3개의 블록, 즉 측정변수블록(MVB), 유도변수블록(DVB) 그리고 명령블록(CB)으로 구분한다. 모든 센서는 측정변수블록의 일부이며, 그 블록은 신호처리를 위한 증폭기, 기능발생기, 배율기 등을 포함한다. 그 출력신호는 유도변수블록으로 보내지거나 비교기의 출력과 같은 논리신호가 된다. 유도변수블록에는 별도의 계산과정이 포함되어 있으며, OTΔT 또는 OPΔT와 같은 변수를 처리하는 부분이다. 이 블록은 두 개 이상의 측정변수블록에서 오는 신호들을 받아서 별도의 신호처리를 하게 된다. 측정변수블록과 유도변수블록의 출력신호가 논리 조작을 위해 명령블록으로 보내진다. 명령블록은 동시성논리에 필요한 다중 채널들 간의 상호 통신에 구심점이 되며, 그 출력신호가 피제어계통 또는 감시 장비들로 보내진다.

3. 주급수 상실시 심층방어 및 다양성 평가

3.1 사건 시나리오

주급수펌프의 정지, 주급수 제어밸브의 닫힘 또는 소외전력의 상실로 인한 주급수 상실사건은 이차측 계통의 열제거능력을 감소시킨다. 이때 원자로가 트립되지 않으면 갑작스러운 열침원의 상실로 인해 노심 손상을 유발할 수 있다. 또한 원자로 트립 후에도 대체급수 공급이 이루어지지 않는다면 노심의 잔열로 인해 상당량의 원자로냉각수가 가압기 방출밸브를 통해 방출될 것이며, 결과적으로 노심의 손상을 초래하게 된다. 이와 같은 과도현상은 열원과 열침원 간의 균형이 깨지므로써 발생하는 것이다. 즉 증기발생기의 주급수가 중단되면 원자로의 출력이 이차측 계통의 열제거 능력보다 크게 되어 원자로냉각재계통(RCS) 온도와 압력을 상승시키며 원자로냉각수를 가압기 쪽으로 밀어 올리게 된다. 이때 이차측 계통에 상당량의 냉각급수가 보충되지 않으면 증기발생기는 끓어 고갈되고, 열제거능력이 완전히 상실됨에 따라 가압기는 완전 충수되며 원자로 냉각재계통의 압력은 급격히 상승하게 된다.

3.2 원자로 보호계통의 기능

원자로 보호계통은 주급수 상실에 대비하여 증기발생기 열전달능력이 감소되기 이전에 그리고 원자로냉각재계통이 핵비등이탈(DNB) 조건에 접근하기 이전에 적절히 자동으로 원자로를 트립하여야 한다. 그림 2와 같이 주급수 상실사건은 일차적으로 증기발생기 저-저 수위에 의한 원자로 트립신호로서 종결되며 그 이차변수로는 가압기 고압력 또는 고수위에 의한 원자로 트립기능이 있다. 고리 1호기에는 증기/급수유량 불일치 트립변수가 추가되어 있다. 안전성분석보고서 제15장에는 주급수 상실 후 대략 1분 경에 보조급수펌프가 자동 기동하여 축적열 및 잔열을 제거함으로써 원자로냉각재계통의 과압 및 냉각수 유출을 방지할 수 있는 것으로 평가되어 있다.

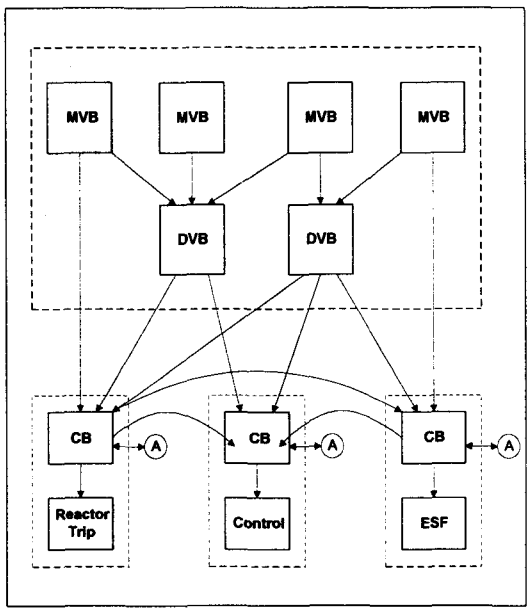

그림 1. 계측채널 블록

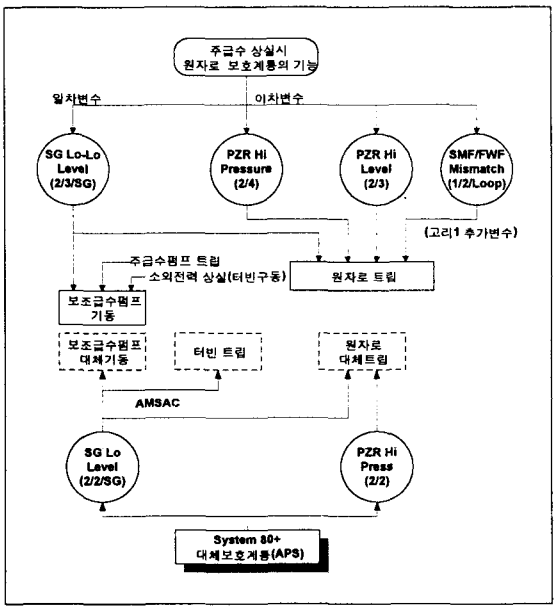

그림 2. 주급수 상실시 원자로 보호기능

3.3 컴퓨터-기반 원자로 보호계통의 다양성 평가결과

그림 2의 트립기능들을 컴퓨터-기반 설계로 구현할 경우 각 변수의 다중 채널들을 블록개념에 따라 측정변수블록, 유도변수블록, 그리고 명령블록으로 나눌 수 있다. 예로서, 공정보호계통의 측정 또는 유도변수 블록들을 컴퓨터-기반시스템으로 설계한 경우 다양성 평가에서는 동종의 블록들에서 공통모드고장을 가정하고, 그 고장에 영향을 받지 않을 대체 블록 또는 기능들을 찾아서 규정된 안전기능을 수행할 수 있는지를 확인한다. 따라서 주급수 상실시 컴퓨터-기반 블록들의 다양성 평가를 위해 동 블록들의 공통모드고장을 가정할 경우, 증기발생기 저-저 수위에 의한 원자로 자동트립과 보조급수펌프 자동기동이 상실되는 것으로 나타난다. 이 경우에도 이차변수들이 트립조치를 취할 수도 있지만 이것들 역시 동일한 하드웨어와 소프트웨어를 사용한 경우에는 일차변수와 동일하게 다중 채널들의 공통모드고장으로 인해 트립기능을 상실한 것으로 가정하여야 한다. 그에 따른 대체수단으로는 ATWS 완화설비가 있을 수 있으며, 동 설비를 갖춘 System 80+의 대체보호계통(APS)과 동 설비가 없는 국내 가동중인 W형 원전(예, 고리 1호기)의 공정보호계통 설비개선사례를 정성적으로 상호 비교·평가한 내용은 다음과 같다.

3.3.1 대체보호계통(APS)가 있는 경우[6]

대체보호계통(APS)은 원자로 보호계통과는 완전히 다르게 가압기 고압력 또는 증기발생기 저수위에 의한 대체트립기능과 증기발생기 저수위에 의한 비상급수펌프 대체기동기능을 갖추고 있다. 주급수 제어밸브의 닫힘으로 인해 주급수 상실사건이 발생하였을 경우 APS는 가압기 고압력에 의한 원자로 대체트립기능을 수행한다. 또한 주급수펌프의 정지로 인해 동 사건이 발생하였을 경우 사건초기에는 원자로출력감발계통(RPCS)이 원자로 출력을 감발시켜 RCS 압력 및 온도의 상승을 억제할 수 있지만, 계속해서 증기발생기 수위가 떨어지고 가압기 압력이 상승하며 표 1에 나타낸 바와 같이 APS가 가압기 고압력에 의한 원자로 대체트립기능을 수행하게 될 것이다. 한편 APS는 위와 같은 안전기능 외에도 증기발생기 저수위에 의한 비상급수펌프의 대체기동기능과 터빈 트립기능을 수행한다. 터빈 트립은 증기유량을 감소시키며 이에 따라 증기발생기의 증기압이 상승하지만 이때 증기우회제어계통(SBCS)이 작동하여 발전소를 고온 무부하상태로 안정시키게 된다.

3.3.2 ATWS 완화설비가 없는 경우[7]

국내 가동중인 W형 원전의 공정보호계통 설비개선사례에 대한 다양성 평가에서는 주급수 상실시 일차 트립변수인 증기발생기 수위채널의 공통모드고장이 원자로 트립과 보조급수펌프 자동기동을 동시에 상실시키는 것으로 나타났다(표 1참조). 이차변수들에 의한 트립기능 역시 동일한 공통모드고장으로 인해 수행될 수 없으며, 이 사건에 대비하여 보조급수펌프를 자동 기동시킬 다양한 대체신호가 마련되어 있지 않다. 만약 어떤 대체급수가 이루어지지 않으면 노심의 잔열은 RCS의 온도를 상승시킴으로써 원자로냉각수를 팽창시켜 가압기를 통한 냉각수의 방출이 예상된다. 따라서 이러한 안전기능상의 취약점을 보완하기 위해서는 컴퓨터-기반 안전설비의 공통모드 고장에 대비해서 원자로 트립과 보조급수펌프 기동에 대한 대체수단이 강구되어야 한다.

표 1. 주급수 상실시 컴퓨터-기반 원자로 보호계통의 다양성 평가결과

구 분 / CMF 그룹		DVB-1	DVB-2	DVB-3	DVB-4	비고
원자로 트립/작동 변수						
1 가압기-고압력		o				
2 가압기-고수위			o			
3 증기발생기 저-저 수위				o		
4 증기유량/급수유량 불일치					o	
완화기능						
W형 국내 가동원전	원자로 자동트립	o	o	o	o	
	보조급수펌프 자동기동	N/A	N/A	o	N/A	
CE System 80+	원자로 자동트립	APS(*)	o	APS(*)	N/A	
	비상급수펌프 자동기동	N/A	N/A	APS(*)	N/A	

주 석

1. DVB는 유도변수블록이며, 컴퓨터-기반모듈을 의미한다.
2. o표시는 완화기능이 관련 컴퓨터-기반모듈의 공통모드고장으로 상실됨을 의미한다.
3. N/A는 적용되지 않음을 의미한다.

* APS는 ATWS 완화설비이다. 또한 발전소 자동제어계통, RRS/RPCS, PLCS, 그리고 SBCS 등도 가용하다.

3.4 컴퓨터-기반 계측제어계통의 심층방어 평가결과

컴퓨터-기반 계측제어계통의 심층방어평가에서는 관련규제기준에 따라[4,5] 안전성분석보고서 제15장 각 사건에 대해서 제어계층, 원자로 트립계층, 공학적 안전설비 작동계층, 그리고 감시 및 표시계층 중에서 최소한 두 개의 독립된 계층들이 가용함을 입증하여야 한다. 만약 가상된 공통모드고장이 어떤 안전기능을 상실시킬 수 있다면, 그와 동일한 안전기능 또는 다른 동등한 기능을 수행해 낼 수 있는 다양한 대체수단을 강구하여야 한다. 만일 비안전성 디지털 또는 아날로그 계통이 관련된 사고조건에 필요한 기능들을 수행할 수 있을 만큼 충분한 품질을 갖추었다면 이러한 계통으로도 다양한 대체수단으로서 고려될 수 있다.

System 80+의 원자로 보호계통과 제어계통은 서로 다른 설계기법과 프로그래밍을 사용하기 때문에 상호간에 다양성이 유지되는 것으로 평가된다. 따라서 컴퓨터-기반 원자로 보호계통이 완전히 상실되더라도 비안전성 대체보호계통(APS)과 감시 및 표시설비가 여전히 가용하며, 주급수 상실시 최소한 독립된 두 계층들을 확보하였으므로 수락 가능한 설계인 것으로 평가된다.[8]

한편 고리 1호기 공정보호계통 설비개선은 보호계통과 제어계통이 동종의 장비와 설계기법을 사용하였고, ATWS 완화설비가 마련되지 않았다. 이 경우 컴퓨터-기반 원자로 보호계통의 기능이 공통모드고장으로 완전히 상실되면 감시 및 표시설비만이 가용하므로 독립된 두 계층들을 확보하지 못한 것으로 평가된다. 그렇지만 10CFR 50.62[9]에 따른 ATWS 완화설비, 즉 ATWS 조건하에서 보조급수펌프의 자동기동과 터빈 자동트립을 위해 센서출력에서부터 최종작동장치에 이르기까지 원자로 보호계통과는 완전히 다른 설비를 갖추면 System 80+와 같이 독립된 두 계층들을 확보하게 되고 원전의 안전성에도 크게 기여할 것으로 평가된다. 특히 국내 가동중인 W형 원전의 공정보호계통 설비 개선시에 CE형 ATWS 완화설비를 추가할 경우, 표 2에 나타낸 바와 같이 6개의 사건에 대해서 컴퓨터-기반 원자로 보호계통의 기능이 상실되더라도 동 설비가 원자로 대체트립 및 보조급수 대체기동을 개시할 수 있으므로, 다양성 확보뿐만 아니라 심층방어 계층요건을 만족할 수 있을 것으로 평가된다.

표 2. ATWS 완화설비의 대체 트립 및 기동기능

제15장 사건 유형	ATWS 완화설비에 의한 대체기능		비 고
	가압기 고압력	증기발생기 저-저 수위	
Uncontrolled Rod Cluster Control Assembly Bank Withdrawal from Subcritical Condition	대체트립	대체트립/보조급수기동	공통모드고장에 의한 보호계통의 기능상실 가정
Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power	대체트립	N/A	
Loss of External Load and/or Turbine Trip	대체트립	대체트립/보조급수기동	
Loss of Normal Feedwater	대체트립	대체트립/보조급수기동	
Loss of Offsite Power to Station Auxiliaries	N/A	대체트립/보조급수기동	
Single Reactor Coolant Pump Locked Rotor	대체트립	N/A	

4. 결 론

CE System 80+ 컴퓨터-기반 보호계통과 국내 가동중인 W형 원전의 공정보호계통 설비개선에 대한 정성적 다양성 및 심층방어 평가결과를 비교해 볼 때 ATWS 완화설비가 결정적인 역할을 하고 있다. 이것은 컴퓨터-기반 계측제어계통이 공통모드고장을 일으킬 수 있는 프로그래밍 설계 오류와 환경영향에 취약하다는 점을 감안하면 필수적인 것으로 평가된다. 따라서 국내 가동중인 W형 원전들도 그 가동년수가 증가됨에 따라 외국 원전들과 유사한 노후화 및 예비품 확보 등의 문제점을 안고 있으므로 아날로그설비를 디지털설비로 교체하는 것이 불가피하며, 그에 따른 설비개선시 ATWS 완화설비를 설치하여 원전의 안전성을 향상시키는 것이 바람직하다고 평가된다.

참고문헌

[1] NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System", NRC, Jan. 1979

[2] NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems", LLNL, Dec. 1994

[3] SECY-91-292, "Digital Computer Systems for ALWRs", NRC, Sep. 1991

[4] SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs", NRC, Apr. 1993

[5] BTP HICB-19, "Guidance for Evaluation of D-I-D and Diversity in Digital Computer-Based Instrumentation and Control Systems", NRC, Jun. 1997

[6] CESSAR-DC, Chapter 7, "Instrumentation and Control", Apr. 1991

[7] I-700-J406-001, "Diversity and D-I-D Analysis for Kori NPP Unit 1", Feb. 1998

[8] KINS/AR-541, "컴퓨터-기반 원자로 보호계통의 심층방어 및 다양성 규제기술 개발", 한국원자력안전기술원, 1998. 4

[9] 10CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for LWRs", Jul. 1996