원자력 발전소 계측제어 시스템

Instrumentation and Control Systems for Nuclear Power Plants

글 | 具仁守
(Koo, In Soo)

산업계측제어기술사
한국원자력연구원 책임연구원

E-mail : iskoo@kaeri.re.kr

At the end of last year, Korean nuclear power plants, APR-1400 and a research reactor have been contracted to build plants at United Arab Emirates and Jordan. Since 1959, a historical background of nuclear technologies in Korea is summarized. The safety requirements for Instrumentation and Control (I&C) systems in Nuclear Power Plants (NPP) are discussed. Specific descriptions on the typical safety classification of I&C systems, the definitions of the electrical class 1E and the countermeasures against common caused failures are provided. And summaries of typical I&C systems such as the protection systems, the control systems, the instrumentations, the monitoring systems and a control room in NPP are introduced. Strict requirements on the development of the digital computer systems in nuclear applications are described.

1. 배경

지난해 연말은 한국 원자력 산업계의 큰 경사가 겹친 해이다. 10월 28일 원자력 산업계 처음으로 원전 통신망 국제 표준이 발간되는가 싶더니, 12월 17일에 아랍 에미리트 연합에서 한국 APR-1400 네 호기의 수출 계약을 완성하였다. 요르단 연구용 원자로 수출이 12월 4일 최우선 협상 대상자로 선정 된 뒤, 2010년 1월 10일 요르단은 한국 컨소시엄을 최종 낙찰자로 선정했다.[1)]

원자로는 우라늄 핵분열 과정에서 발생하는 열을 이용해서 전력을 생산하는 발전용 원자로(APR-1400과 같은 상용 원전)와 핵분열 시 생성되는 중성자를 활용해서 여러 가지 연구를 수행하는 연구용 원자로로 볼 수 있으며, 발전용 원자로는 국가의 필요한 에너지원을 전력을 통해 공급하는 국가의 에너지 확보 및 온실가스 감축에 대처하는 현실적 수단이다. 연구용 원자로는 중성자 산란 장치를 이용한 물질의 구조 연구 및 신물질 개발 등 중성자 과학, 의료용 및 산업용 방사성동위원소 생산, 핵연료와 원자로 구조재 등 재료의 안전성과 건전성을 시험하는 조사시험 등에 다양하게 활용한다.

1959년 7월 서울 공릉동에서 한국 최초의 원자로인 연구용 원자로 트리가 마크 II[2)]기공식이 있었다. 이를 기점으로 우리나라는 원자력 에너지의 이용에 첫 시작을 알린 셈이다. 이후 1978년 한국 최초의 원자력 발전소인 고리 1호기가 일괄 공급형태로 가동을 시작함으로써 원자력 에너지를 산업 동력으로 사용하기 시작했다. 당시 세계에서는 1979년 3월 미국의 TMI사고, 1986년 4월 구 소련의 체르노빌 사고 등으로 인해 원자력 발전소 건설이 거의 중단되었다.

그러나 우리나라는 부존자원의 결핍으로 인한 에너지 안보와 관련하여 원자력 발전소를 계속적으로 건설하였으며, 특히 지난 2009년 초 세계를 뒤흔들었던 살인적인 원유가 상승, 이제까지 무한이라 믿었던 대량 에너지원인 세계의 석유 부존자원은 이미 peak-oil 상태를 넘어섰다. 반면에 바이오-연료와 태양광, 태양열, 풍력, 지열, 조력, 수소연료, 연료전지, 핵융합 등 다양한 분야의 대체 에너지 개발에 세계가 매우 노력하고 있으나, 인류가 필요한 대량의 에너지를 공급할 대체 수단으로 원자력 에너지가 어쩔 수 없는 선택이며 저탄소 배출 친환경 에너지임을 인식하고 있다.

우리나라는 현재 20개호기가 가동 중에 있으며, 6개호기가 건설 중이며, 6개호기가 추가 건설 계획 중이다.

세계 원자력 energy의 주 공급 수단은 원자력 발전소에 의한 전기 생산이다. 현재 세계에 438호기의 원전이 가동 중이며, 47개호기가 건설 중이다.[3)]

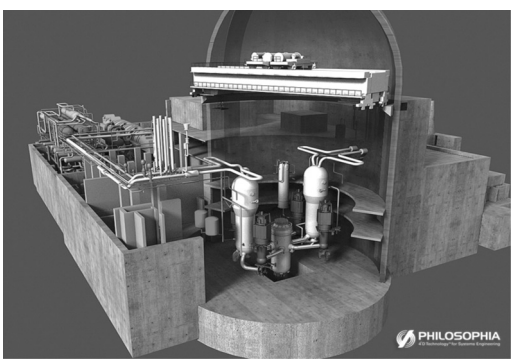
이와 같이 향후 2030년도까지 세계는 국가 에너지 확보 수단으로 원전을 대량 건설할 예정이며, 트리가 마크 II 연구용 원자로 이후 약 50년 동안 원자력 산업계의 기술적 노력에 힘입어 이제는 수출산업의 한 축을 담당한다. 원자력 플랜트의 건설은 모든 산업분야의 파급효과가 지대하여 고부가 가치 상품이라 할 수 있다.

원전 기술자립[2)]

1980년대 초반부터 한국핵연료 주식회사와 한국원자력연구소를 중심으로 핵연료 국산화 개발, 한국원자력연구소를 중심으로 1980년대 중반 표준원전 설계사업, 기술전수 계약 등을 통해 국산화 기반을 다졌으며, 1989년 2월 처음으로 한국원자력연구소 설계, 한국핵연료 주식회사가 제작한 최초 국산핵연료를 장전했다. 이후 영광 3,4호기의 핵연료는 한국원자력연구소가 당시 미국 Combustion Engineering사(현재 Westinghouse에 합병됨)와 공동설계로 개발하고, 표준원전인 울진 3,4호기는 독자로 설계했다. 1986년 말 Combustion Engineering 사와 발전로 계통 국산화를 위해 공동설계에 착수하였으며, 울진 3,4호기부터는 한국주도로 설계를 수행하였다. 이런 일련의 기술자립에 대한 노력의 결과로 울진 3,4호기는 우리 한국 기술진의 주도로 완성한 원전이다. 한국형 표준원전 1호기인 울진 3,4호기는 설계수명 40년, 핵연료 열적 여유도 5%이상을 확보하고 한국의 인간공학적 개념을 적용한 최신 제어설비로 인적 오류를 저감 화하였으며, 기술도입 모델인 System80+ 원전에 비해 크게 설계 개선하여 안전성과 신뢰성을 증진시켰다.

차세대원전(APR-1400) 개발[2)]

차세대 원전은 한국 표준원전의 연장선상에서 미래 노형 개발 전략으로 논의를 시작하였으며, 1992년 국가 G7과제로 APR-1400 개발을 시작하였다. 1단계 사업은 1992년 말부터 1994



▲ 한국형 표준원전 투사도

년까지 원자로형과 설계개념을 확정하였으며, 노심출력 4,000MWt급, 설계수명 60년, 노심 손상빈도 10^{-5}/년 이하, 격납건물 건전성 상실빈도 10^{-6}/년 이하, 가동률 90%이상, 건설공기 48개월 등이며, 설계원칙으로 설계 단순화, 충분한 설계 여유도 확보, 인간공학 기술 적용, 입증기술 사용 등이었다. 2단계 사업은 1995년부터 1999년 초까지 수행하였으며, 설계개선 사항 중 10개의 피동 안전개념을 적용하였다. 1999년부터 2002년까지 3단계 사업으로 설계인증을 받기위한 연구, 개발업무를 수행하였으며, 입증기술 확보에 많은 노력을 기울였다. 금번 아랍 에미리트 연합에 공급하는 APR-1400은[1] 이런 과정을 거쳐 국내 신고리 3,4호기와 신울진 1,2호기가 2013년부터 2016년까지 순차적으로 완성될 것이다. 참고로 이번 수주한 원전의 첫 호기가 아랍 에미리트 연합의 살라지역에 2017년 5월까지 준공 목표이다.

2. 원전 계측제어 관련 안전원칙

국제원자력기구(IAEA) 안전원칙의[4] 목적은 방사선 피폭에서 인명과 환경을 방호한다.

이를 위해 안전 책임, 정부 역할, 안전 경영, 방사선 시설 및 업무 정의, 방호 최적화, 개인 위해 제한, 세대 간 위해 방호, 사고 방지, 방사선 사건에 대한 비상 대비, 방사선 위해 저감 방호 행위 등 10개의 안전원칙을 명문화 하고 있다.

국제원자력기구의 안전요건은[5] 방사선 방호 목적과 기술적 안전 목적을 달성하기위해 심층방호 요건인 6개 준위의 방호 개념을 가져야한다. 계측제어는 제어, 보호, 공학적 안전설비 작동, 안전 감시 및 비상대응 등으로 이루어진다.

안전 등급 분류, 일반 설계 기준과 공통 원인 고장, 단일 사고 기준, fail-safe 설계 등과 같은 신뢰성 확보, 시험, 보수 유지, 검사 및 감시 기능 완비, 기기 검증, 갱년 대처, 인간공학 적용, 안전 해석 등 안전 확보를 위한 설계요건을 적용한다.

원전 계측제어의 상위 요건으로 정상운전, 비정상운전 등 모든 운전상태의 원전 변수를 감시하는 계측, 과냉각 여유 측정의 자동 기록, 적절한 제어 수단 등 일반요건과 제어실, 이차 제어실, 컴퓨터 기반 계통, 자동제어, 보호 기능, 보호 기능과 제어 기능의 분리 등과 같은 특정 요건, 비상 제어 센터, 비상 전원, 방사선 방호 등에 필요한 기능을 명시한다.

우리나라는 원자력법, 시행령, 시행규칙, 원자로 시설 등의 기술기준에 관한 규칙 및 방사선 안전관리 등의 기술기준에 관한 규칙 등에 명시되어 있다.

이를 근거로 안전성에 관한 엄격한 요건에 따라 원자력 발전소에 사용하는 모든 설비 및 행위는 별도의 인허가 기관의 규제 하에 법적으로 아주 엄격한 과정을 거쳐 안전성을 확립한다.

가압 경수로[6]

우리나라는 주로 가압 경수로이며 월성 원전 네 개호기만 냉각재로 중수를 사용하는 CANDU형 원자로이다.

가압 경수로는 1차계통의 냉각재에 경수를 사용하며, 1차 계통의 온도는 약 315도, 압력은 15MPa 정도이다. 1차 계통의 가열된 물은 2차 계통의 물을 포화 수증기로 만들어 증기 터빈으로 보낸다. 가압 경수로는 연쇄반응을 유지하기 위해 빠른 중성자의 속도를 낮추며, 이는 가압 경수로의 중요한 안전장치이다. 원자로의 출력 제어는 제어봉과 붕산농도 조절이라는 수단을 사용한다.

가압 경수로의 주요부품은 핵연료, 원자로, 가압기, 냉각재, 냉각재 펌프, 증기발생기, 격납용기, 터빈-발전기 등으로 구성되며, 핵연료, 원자로, 냉각수, 격납용기 등으로 심층방호 개념을 달성하고 있다.

3. 원전 계측제어 안전 요건

가. 일반 요건

원전의 계측제어 설비는 크게 안전에 중요한 기기와 중요치 않은 기기로 분류하고, 안전에 중요한 기기는 안전 계통과 안전 관련 계통으로 분류한다.

안전 계통은 원자로를 보호하기 위한 각종의 계측제어 설비가 자동 작동하는 보호 계통과 안전 설비 작동 계통 및 안전 설비 지원 계통으로 구성한다.

나. 특정 요건

원전의 인적 오류를 극소화하기 위해 설계 초기 단계부터 설계, 구현, 소프트웨어, 인간기계 연계(man-machine interface), 각종 절차서, 비상 계획 등 인적 요인이 개입하는 모든 요소에 대해 체계적인 설계 방법을 적용한다.

특히 원전의 상황을 인지하는 데 장애 요소를 제거하여 사건 발생 시에 신속히 원전 상태를 파악하여 인적 오류 발생이 없도록 한다.

안전 기능의 대처는 인적 오류 발생 가능성이 높은 비상 상태이므로 일정기간 동안 운전원의 개입없이 자동으로 원전이 안전 행위를 하도록 제한한다. 능동형일 경우 보호계통이 완전 자동화 되어있으므로 30분이내 운전원의 제어 행위를 제한한다.

따라서, 운전 조치 행위를 최소화하여 운전 요원의 업무 부담을 줄이고 인적 오류 발생을 줄인다.

시각 정보 표현과 계측 및 경보는 가용 시간, 예상하는 물리적 환경 조건과 정신적 부하 등의 제한 하에 운전 요원이 성공적인 조치 행위를 하도록 지원한다.

원자로 제어는 원자로가 미 임계에 도달하고, 기동, 출력 운전 등 모든 운전 상태와 설계 기준 사고에서 미 임계를 유지하는 충분한 부 반응도 제어가 가능해야 한다. 제어 계통 고장을 포함한 설계 기준 사고에서도 원자로 정지 능력이 있어야 한다.

원자로 특성에 따라 자동정지 계통을 원자로 정지계통과 사고 완화를 위한 공학적 안전설비 작동계통을 둔다. 원자로 정지 계통의 효용성, 조치 반응 속도 및 정지 여유도는 지정한 한계치와 조건을 부합한다.

제어봉 고착 등 정지 계통의 단일 고장에도 안전 기능 작동이 필요할 때에 수행에 지장이 없다.

비상 정지에 적합한 하나 이상의 수동 정지 개시 행위를 할 수 있는 수단을 마련한다.

원자로 운전의 모든 상태에서 계측 기기는 정지 수단의 건전성을 확인하는 시험을 할 수 있으며 항상 감시 가능하다.

원자로 보호 계통은 자동으로 기능을 수행하며, 다른 어떤 계통과 독립성을 보장한다. 동시에 수동 원자로 비상 정지 신호가 원자로 보호 계통의 입력으로 사용한다.

전 범위의 예상 가능한 개시 사건에 대해 안전하게 그 사건을 종결하는 데 필요한 보호 조치는 자동으로 이루어진다. 계통의 일부에서 발생 가능한 오작동 등 단일 고장 요건을 원자로 보호 계통 기능에 반드시 고려하여 설계한다.

충분히 신뢰할 수 있는 조건하에 운전 요원이 수동 조치가 가능할 수 있다.

원격 장소에서 원자로 정지를 개시할 수 있는 기능을 부여한다.

원자로 보호 계통은 단일 고장 발생이 자동 보호 기능 작동에 영향이 없게끔 다중성과 독립성을 가진다. 원자로 보호 기능의 상실을 방지하기 위해 failsafe 특성과 다양성 확보와 같은 설계 기법을 적용한다. 이 보호 기능은 자동으로 관련 기능을 개시한다.

원자로 보호 계통이 하드웨어고장, 갱년 열화로 인한 고장이나 인적 오류가 발생하더라도 원자로를 안전한 방향으로 작동시키고, 안전 상태를 유지토록 설계한다. 원자로 보호 계통의 모든 부품은 기능 시험을 해야 하며, 계측의 정확도, 교정의 불확도, 계측기 드리프트, 응답 시간 등 충분한 여유도를 갖도록 설정치를 설계한다.

컴퓨터기반 원자로 보호 계통을 증명하기 힘들 때 실배선 등과 같은 보호 기능 수행이 확실한 다른 수단을 준비한다.

각종 지시 및 계측은 제어실에 집중 배치하며, 예상 운전 과도 상태나 사고 시에도 운전 요원을 보호하는 적절한 수단이 있다.

4. 원전 계측제어 특성 및 구조

가. 원전 계측제어 특성

1) 등급 분류[7]

계측제어의 등급 분류는 그 안전성 측면 중요도에 따라 각 나라별로 상이하다. 우리나라는 전기안전등급을 적용하며, 최근 디지털 시스템의 적용으로 소프트웨어 안전성과 관련하여 계측 등급 I, II, III의 분류 방식 도입을 추진 중이다.

2) 전기 안전 등급 1E 요건

원전의 설계기준사건에 대비하여 안전기능을 수행하는 원자로 정지계통, 노심보호계통, 공학적 안전설비 작동계통, 안전정지계통의 계측설비, 안전 관련 정보 및 연동계통, 안전 관련 자료 통신망, 안전 관련 수동제어 설비, 안전 관련 표시기 및 기록기 등에 적용한다. 이들 계통의 소프트웨어는 안전성 필수 소프트웨어로 분류하며 이는 가장 엄격한 품질 보증요건과 소프트웨어 구성 요소가 안전계통에 미치는 위험도 및 위해도 분석을 통해 공통원인고장 발생 가능성을 배제해야하며, 개발조직과 별도의 기술, 조직, 책임, 권한 및 재정적으로 독립된 확인 검증 조직에 의해 소프트웨어 확인 검증 활동을 해야 한다. 이는 원자로 보호계통 및 안전 관련 계측제어 계통 요건에 부합해야하며, 단일 고장 기준을 만족하고, 환경요건에 따른 환경 검증, 전자파 방출 및 내성 검증, 내진등급 I에 맞는 검증 시험, 심층방호 및 다양성 분석을 수행해야 한다.

3) 공통원인 고장 대처 방안[8]

원전의 안전 관련 계통은 3채널내지 4채널의 다중성을 가지게 설치한다. 여기에, 디지털 시스템의 속성상 공통원인 고장의 가능성을 배제하도록 설계에 다양성을 확보해야 한다. 다양성 유형으로는 인적 다양성, 설계의 다양성, 소프트웨어의 다양성, 기능의 다양성, 신호의 다양성, 기기의 다양성 등으로 볼 수 있다. 인적 다양성은 안전 계통에 대해 설계, 개발, 설치, 운전, 유지보수 등의 인적 행위가 아주 다양하므로 서로 다른 사람이 같은 종류의 행위를 하므로서 인적 오류를 저감한다. 설계의 다양성은 설계에 포함된 유사한 문제를 서로 다른 접근 방법을 사용하여 해결한다. 소프트웨어 다양성

은 설계, 구현 등에서 같은 소프트웨어 기능을 서로 다른 개발자나 집단이 개발한다. 기능의 다양성은 두 개의 계통을 물리적으로 서로 다른 기능으로 완성한다. 신호의 다양성은 보호 기능의 작동을 서로 다른 신호 변수를 이용한다. 기기의 다양성은 유사 안전 기능에 서로 다른 제작사의 기기를 사용하는 것 등이다. 이와 같은 요건에 부합성을 분석하여 다양성 확보를 확인해야 한다.

나. 세부 계통의 기능

1) 보호계통

보호계통은 크게 노심보호계통, 원자로 보호계통과 공학적 안전설비 작동계통 등이 있다. 노심보호계통은 노심을 감시하고, 임계출력비율 및 선출력밀도를 계산하여 예비정지설정치와 비교하여 예비정지신호를 생성하고, 정지설정치와 비교하여 원자로 정지신호를 생성하는 기능, 예비정지신호 및 제어봉 집합체 편차 등이 발생할 경우 제어봉 집합체 인출금지신호 생성하는 기능을 가진다. 대체로 이 노심보호계통의 입력신호는 냉각재 펌프 속도, 고온관 온도, 저온관 온도, 가압기 압력, 노외중성자속, 각 제어봉 위치 등이다. 원자로 보호계통은 바이스테이블, 동시논리, 제어봉 개시, 공학적안전설비 작동 개시, 시험 기능 등으로 구성된다. 바이스테이블 기능은 노심출력, 압력, 수위 또는 온도 등에 대한 측정변수 값이 설정치를 초과하면 정지신호를 발생한다. 이 정지신호는 동시논리 기능으로 입력되며, 원자로 정지 개시기능으로 신호를 보낸다. 원자로정지 개시기능은 원자로정지차단기에 원자로정지신호를 내보낸다. 공학적안전설비 작동 개시기능은 안전등급제어계통으로 안전통신망을 통하여 보낸다. 안전기능이 필요없는 운전모드에서는 원자로정지를 막기 위해 개시기능을 우회한다. 시험기능은 한 번에 한 채널씩 시험하기 위해 원자로 보호기능을 우회한다. 채널우회, 운전우회와 가변설정치의 리셋 등과 같은 인간기계연계를 위해 운전원 모듈이 설치되며, 보호계통의 시험기능을 보수시험반을 갖는다. 시험기능은 자동시험과 수동시험 기능을 갖는다. 자동시험 기능은 수동주기 감시시험을 줄이며, 자동시험으로 할 수 없는 시험은 수동시험으로 한다. 원자로보호계통 각 채널의 보수시험반은 보호계통의 운전상태를 감시하고 시험한다. 각 채널은 정보처리계통과 경보지시계통으로 선택된 보호채널상태와 시험상태의 정보를 제공한다. 공학적 안전설비 작동계통은 원자로 보호계통의 신호를 받아 안전주입, 주증기 격리, 주급수 격리, 격납용기 살수, 재순환, 비상 디젤 발전기, 안전급 공기조화계통 등 공학적 안전설비와 관련한 기기 및 계통에 대한 상태제어나 지속적 조절기능을 가지며, 이는 원자로 보호계통의 작동후 잔열제거 기능도 가진다.

2) 제어계통

제어계통은 출력제어, 공정제어, 이차제어 등으로 구성된다. 출력제어는 제어봉 구동장치 제어, 원자로 출력 급감발 제어 원자로 출력제어, 예비보호제어 등의 계통으로 구성되며 공정제어는 다양성 보호, 정화제어, 급수제어, 증기우회, 기타 BOP(Balance of Plant) 연계 등의 계통으로 구성된다. 이차제어는 터빈-발전기 제어, 복수 제어, 복수기 진공, 순환수 제어, 2차측 냉각수 제어, 2차측 기기냉각수 제어, 기타 BOP설비 연계 등의 계통으로 구성된다.

3) 계측계통

계측계통은 크게 공정계측과 핵계측으로 분류하며, 공정 계측은 발전소 공정계통의 열수력 현상과 기기 상태에 따른 온도, 압력, 유량, 수위, 속도, 위치 등의 변수를 감지하여 신호처리 후 관련 보호, 제어 및 감시 계통의 입력으로 연결된다. 핵계측은 대체로 노외중성자속 계측과 노내중성자속 계측으로 나누며, 노외 중성자속은 열중성자속을 측정하기위해 비보상 전리함, 보상전리함, 핵분열함 등을 사용한다. 최근에는 광역 핵분열함을 채택하고 있다. 노내 중성자속 계측은 원자로 출력시 원자로의 노심 내부의 중성자 출력분포를 감시하기 위해 설치하며, 축방향과 원주방향으로의 열중성자속 분포를 상시 감시한다.

4) 감시계통

감시계통은 크게 사고후 감시 지시, 일차측 건전성감시, 노외 중성자속 감시, 발전소 상태 감시로 볼 수 있으며, 사고후 감시계통은 발전소 사고후에도 지속적인 감시가 가능해야하며 노심 출구온도, 부적절 노심냉각, 열중성자속 등 주요 변수에 대한 상시감시가 발전소 사고후에도 가능하다. 일차측 건전성 감시는 크게 열중성자속 신호를 이용한 원자로내 진동감시, 가속도계를 이용한 금속파편 감시, 음향방출신호를 이용한 주요 배관이나 안전방출 밸브 개폐상태를 감시하는 음향방출 감시, 냉각재 펌프 상태 감시 등으로 일차측 주요 기계부품의 건전성을 실시간으로 감시하는 기능이다. 노외 중성자속 감시는 원자로 출력을 감시하는 주 수단으로 발전소 전체 운영과 관련하여, 정상, 비정상 및 사고와 관련한 주요 감시수단이다. 발전소 상태감시는 발전소 주전산기 계통과 경보계통으로 구성되며, 운전원의 사전 인지를 위해 가청 경보, 시각 경보 등을 사용한다. 전산기 계통은 발전소 모든 상태를 입력으로 발전소의 상태를 감시하고 기록하며 최적의 정보 표시기법으로 운전원 행위를 위한 정보 전달 기능을 수행한다.

5) 제어실

제어실은 정상운전시 상시 거주하는 주 제어실과 주 제어실 접근 불가능시 사용하는 원격정지실이 있다. 제어실은 발전소의 안전을 확보하고 성능을 보장하기위한 공정 및 안전기능을 상시 감시하고 적절한 제어를 위한 운전행위 수단을 갖추고 있다. 대체로 주 제어실은 주 제어반, 안전 정지 제어반, 보조 제어반, 감독자 감시반, 화재 작동 설비, 자료실, 회의실, 비상지원실 등을 갖추고 있으며, 각 제어반에는 운전을 위한 모든 정보를 파악할 수 있도록 설계된다.

다. 안전계통의 디지털 컴퓨터 개발

디지털 컴퓨터의 발전소 안전 계측제어계통 적용은 공통원인 고장을 유발할 가능성이 아주 높다. 따라서, 하드웨어 고장보다 다중 채널의 소프트웨어 설계 오류, 개발 오류, 구현 오류 등의 가능성이 매우 높다. 따라서 소프트웨어 품질보증과 확인검증이 매우 중요한 활동이다. 이외에 다양성 확보와 같은 추가 보완 수단을 마련해야 한다. 4. 가. 3)항에서 기술한 공통원인 고장 대책으로의 다양성 확보와 심층방호의 다양한 수단이 적용된다.

구현과 관련한 모든 구성품은 반드시 다양성 분석을 통해 그 만족성을 확인한다. 소프트웨어는 다양성 만족에 회의적이므로 기능 및 신호의 다양성을 소프트웨어 개발시작부터 반영한다. 소프트웨어의 개발은 폭포수 모델인 소프트웨

어 생명주기에 따라 개발, 확인 검증, 안전성 분석 등 소프트웨어에 내재될 수 있는 취약성을 제거한다. 동시에 사이버 보안 요건을 설정하고 그 만족성 여부를 각 단계별로 확인한다.

5. 결론

원전의 계측제어계통은 발전소의 신경으로서 모든 안전과 성능에 직접적인 영향을 미친다. 최근 적용하는 기술인 디지털 컴퓨터 기반의 안전계통은 매우 엄격한 요건과 구현과정, 확인 검증 과정을 거쳐서 설치, 유지되므로 원전은 일반 계측제어 시스템이 설치된 플랜트에 비해 매우 안전하다고 하겠다.

최근 원전 계측제어를 뒷받침하는 IT산업의 비약적인 발전으로 인해 디지털 시스템의 외부로 부터의 위해성이나 자체의 취약성은 점증되는 현실이다. 따라서, 이런 위해성이나 취약성을 제거하기 위한 일련의 활동이 원전 계측제어계통 개발의 주된 요소 업무라해도 과언이 아니다.

동시에 정량적 평가기법을 동원하여 새로운 소자나 기기, 기법에 대해 위해성 평가를 수행하여 그 결과에 따라 보완 수단 마련이나 보완 시스템을 설치한다. 디지털 컴퓨터 시스템의 이런 속성 때문에 온도, 습도, 먼지 등 주위 환경에 대한 하드웨어 검증, 지진이 발생하더라도 계통의 기능을 상실하지 않도록 설계하며 설치 전에는 반드시 내진검증 시험을 통과해야한다. 특히, 격납용기 내부에 설치하는 모든 기기나 센서, 전선 등은 반드시 방사선 피폭에 대한 환경 검증을 받은 제품만이 가능하다. 이와같이 일부 안전 계통의 소자는 가혹 환경에서의 운전 이력 등 안전성 증명을 위해 일반 계측제어 산업에 비해 매우 많은 추가 업무를 수행한다.

국내에서 안전 계통에 사용가능한 제어기 생산이 가능하나, 운전 이력의 미진으로 적용이 되지 않은 것은 약간의 아쉬움이 있다. 그렇지만 향후 국내 신규 원전에 적용하기로 결정하였으므로 수년내에 이 기술도 수출 전선에 나설 수 있으리라 판단한다. 원자력 적용 기술은 고도의 안전성을 확보해야 하므로 안전성 증명에 보다 많은 투자가 지속적으로 필요할 것이다.

〈원고접수일 2010년 3월 2일〉

■ 참고문헌

1) 원자력 산업회지 2010년 1-2월호
2) 한국원자력연구원 50년사, 2009년
3) IAEA Reactor Data Series No. 1, 2009년
4) IAEA Safety Fundamentals, SF-1
5) IAEA NS-R-1, Safety of Nuclear Power Plants; Design
6) 한국원자력지식정보 관문국, www.atomic.or.kr
7) IAEA NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants
8) Methods for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems, UCRL-ID-119239, Lawrence Livermore National Lab.