원자력발전소 디지탈 계통 설계의 안전성

윤원영

한국원자력안전기술원

1. 머릿말

그동안 지속적으로 발전되어온 디지탈 계통 설계 기술은 산업계의 전 분야에 걸쳐서 다양하게 응용되고 있으며 이로 인한 산업발달의 파급효과는 매우 엄청난 것으로 평가되어 지고 있다. 원자력발전소 설계분야에 있어서도 디지탈 계통 설계 기술의 적용영역은 1970년대 중반 이후 점진적으로 증대되어 왔으며 그중에서도 지난 10년여 동안의 디지탈 설계기술의 적용범위와 중요성은 급격히 증대되고 있는 추세이다. 이와같이 세계 각국의 원자력 산업계가 디지탈 계통 설계분야에 적극적인 기술개발과 실용화를 추진하고 있는 중요한 이유는 다음과 같은 2가지 측면에서 해석되어질 수 있다.

첫째 요인은 기존의 아나로그 계통설계의 한계성을 인식한 대체수단으로서의 역활이라 할 수 있다. 즉, 현재 원자력발전소를 세계에서 가장 많이 보유하고 있는 미국의 경우 운전중인 원자력발전소 계측제어계통 부품의 약 80% 정도가 생산 중단된 상태이며, 이로인한 발전소 운전 및 보수에 상당한 애로를 경험하고 있는 실정이다. 이는 원자력발전소의 주요 구조물과 기계 부품들이 30년이상 비교적 긴 수명을 유지할 수 있는데 비하여 계측 및 제어 부품들은 원전 수명기간중 2~3회의 교체가 불가피한 경우가 대부분이며 이들 부품의 제조업체 입장에서도 급속한 기술개발 등으로 인하여 동일 제품을 계속적으로 생산할 수 없는 문제가 발생되게 된다. 따라서 기존의 노후화된 아나로그 계통설계 내용을 디지탈 계통 설계로 대체할 경우 원전 운전의 경제성을 개선하고 발전소 운전수명을 연장시키는 부수적인 효과를 기대할 수 있을 것이다.

둘째 요인은 1979년 발생된 미국 TMI 발전소 사고 이후 꾸준히 제기되어온 기존 원자력발전소의 안전성에 대한 우려를 불식시키고 원자력 산업의 활로를 모색하기 위한 새로운 차원의 원전 설계 방안으로서의 역활이 되겠다. 즉, 세계 각국의 원자력 산업계는 최근 원자력 설계기술의 혁신을 통한 원자력발전소의 안전성과 경제성을 동시에 증진 시키기 위한 관련 연구 개발을 진행 중에 있으며 이는 다양한 형태의 차세대 원자력발전소 (또는 신형 원자력발전소) 모델로서 나타나고 있다. 이들 차세대 원전의 공통적인 설계 특징중의 하나는 디지탈 계측 및 제어계통 설계의 전면 채택이라 할 수 있다. 이에 대한 주요한 이유는 원전 설계자의 입장에서 볼 때 디지탈 계통설계의 채택의 설계의 단순화와 표준화를 용이하게 하고 운전중 보수유지 측면에서도 많은 장점을 지님으로서 원전 설계 및 운영의 경제성과 편이성을 증대 시킬 수 있을 것으로 기대되기 때문이다. 그럼에도 불구하고 디지탈 계측제어계통 설계에 대한 세계 각국 안전규제 기관의 견해가 다소 부정적이고 유보적인 입장을 견지하는 주요 원인은 디지탈 계통에 내장된 소프트웨어 프로그램에 대한 정량적인 신뢰성 평가가 현 단계에서 불가능하고 소프트웨어 프로그램의 오류로 인한 계통운전의 오동작 (Common Mode Fail) 가능성이 매우 높다는 점이다. 이와 같은 디지탈계통 소프트웨어 프로그램 오류 발생의 가능성과 이로인한 원전 운전 안전성에 미치는 파급효과는 설계자의 입장에서도 예측하기 어려운 점을 인정하고 있는 실정이다. 또한 디지탈 계통 설계시에는 종래의 아나로그계통 설계시에 고려치 않았던 새로운 고장모드에 대한 고려 즉, 전자파 간섭(EMI)에 의한 계통운전의 오동작 발생 등을 추가적으로 고려하여야 한다는 것이 전문가들의 견해이다. 이와 관련하여 국제원자력기구(IAEA)를 위시한 세계 각국의 원자력 안전규제 기관은 원전 디지탈 계통 설계의 안전성을 증진 시키기 위한 새로운 안전규제 기준의 제정과 규제법규의 정비를 추진중에 있다.

본 기고에서는 현재까지 제시된 원전 안전관련 디지탈 계통설계의 개발 현황과 각국의 규제동향 및 안전심사 내용 등을 소개하고져 한다.

2. 안전관련 디지탈 계통의 개발 현황

1) 미국의 경우

일반 산업계에서의 디지탈 컴퓨터 기술의 보급은 다른 나라에 비하여 선구자적인 위치에 있었음에도 불구하고 원자력발전소 설계분야에 디지탈 컴퓨터가 최초로 도입된 것은 1970년대 후반에 Combustion Engineering(C-E) 사에의해 개발되어 Arkansas Nuclear One 원전 2호기 (ANO-2)에 적용된 노심보호연산기(CPC)이다. 노심보호연산기의 주요기능은 운전중인 원자로심의 핵비등율(DNBR) 과 국부 열출력밀도(LPD) 값을 실시간으로 계산하여 사전에 설정된 안전운전 설정치를 초과시 즉각적인 원자로 정지와 관련 조치가 이루어질 수 있도록 하는 것이며 계통구성은 4대의 CPC 컴퓨터와 2대의 보조컴퓨터(CEA 컴퓨터)로 되어 있다.

원전 설계 안전성 측면에서 CPC 의 원전 설계 도입은 당시로서는 미국 원자력 산업계 뿐 아니라 세계 원자력 산업계의 최대 관심사 였다. 미국의 원자력규제위원회(NRC)에서는 CPC 설계의 안전성 평가를 위하여 미국내 컴퓨터 계통설계 분야의 전문가로 구성된 특별심사팀을 별도로 운영하며 약 3년에 걸친 심사를 수행한 바 있다. 또한 최종 운영허가를 발급시에도 이후 CPC 의 고장으로 인한 원자력발전소의 운전정지 또는 이상사태 발생은 즉각 보고하고 원인규명이 될때 까지는 발전소 출력운전을 금지할 것을 허가조건으로 결정하였다. 그러나 NRC에서 우려한 바와같은 CPC 의 이상은 나타나지 않았으며 이후 CPC 의 초기 고장 횟수도 점차 안정화되는 것으로 보고된 바 있다. C-E사에서는 이후에도 San-Onofre 원전 2,3호기와 Waterford 원전 3호기, Palo Verde 원전 1,2,3호기 등에 개선된 설계의 CPC 를 도입하여 그 성능이 우수함을 입증하였다.

이를 계기로 미국 원자력 산업계는 원자력발전소의 설계분야에 디지탈 계통 설계기술을 적극적으로 채택하게 되었으며 1980년대 초반부터 거론되기 시작한 차세대 원자력발전소 설계는 미국 내 대부분의 원자력발전소 설계사가 발전소 제어계통 및 보호계통 구성을 전산화하는 방향으로 설계를 추진 중에 있다. 예로서 C-E사의 차세대 원전 모델인 Nuplex 80+ 설계의 경우 그림 1과 같이 완전 전산화된 계통설계를 개발 완료하여 NRC의 설계인증을 취득하였으며, Westinghouse 사에서도 이와 유사한 개념의 Eagle 21 이라는 종합화된 디지탈 제어 및 보호계통을 개발하여 설계인증을 취득한 바 있다. 또한, Westinghouse 사의 디지탈 제어 및 보호계통은 이미 SPEC 200 Micro Module 이라는 하드웨어를 사용하여 가동중인 Connecticut Yankee Plant, Indian Point 3 Plant, Donald C Cook 1&2 Plant 등에 설치한 바 있다. 이외에도 미국 내 5개 전력회사로 구성된 B&W Owners Group 에서는 EPRI와 공용으로 발전소 제어 및 보호기능을 디지탈화 하는 개선된 발전소 제어계통 (PCS) 개발에 착수하여 현재 개발 완료단계에 도달해 있다. 이러한 원전 사업자들의 디지탈 계통설계 움직임에 대응하여 NRC에서는 안전관련 디지탈 컴퓨터의 규제지침 Reg. Guide 1.152를 제정하고, 이를 통하여 컴퓨터 시스템 개발 과정의 품질보증 활동은 ASME NQA-1에 따라 수행하고 소프트웨어 프로그램의 개발과정에서의 단계별 확인 및 검증활동 및 결과는 IEEE 7-4.3.2에 따라 수행되어져야 함을 밝힌 바 있다. 또한 이후에도 NRC에서는 관련 규제지침 및 정책성명 등을 계속적으로 공포하고 현재도 세부 규제지침 제정을 위한 연구를 진행 중에 있다.

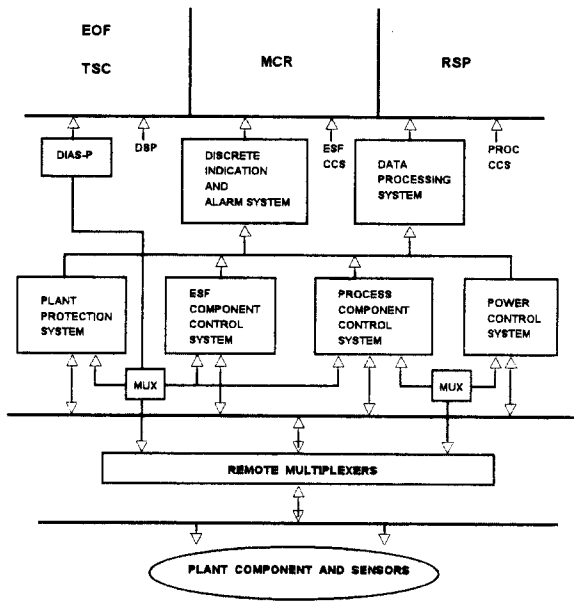


그림 1. Nuplex 80+ System Configuration.

2) 프랑스의 경우

1960년대 초창기의 프랑스 원전인 개스냉각원자로(GCR)의 경우 제어계통 설계시 이미 디지탈 제어계통 설계가 도입된 바 있으나, 현재 주종을 이루고 있는 가압경수로(PWR) 원전의 경우는 1980년대 중반 Merlin-Gerin 사에 의해 개발된 디지탈 원자로 계측 및 보호계통 (SPIN)의 설계 적용이 최초라 할 수 있다. SPIN의 주요기능은 원자로심과 1차냉각계통의 운전변수를 신호처리하여 필요시 원자로를 긴급 정지 시키기 위한 신호를 발생시키는 1E Class 보호계통으로 1300 MWe급 원자력발전소 설계에 채택되어 현재 20기의 원전에 사용되고 있다. 이 후 Merlin-Gerin사에서는 SPIN의 적용 영역과 기능을 개선한 SPIN 2 (P20)

의 개발에 착수하여 1990년 중반 상업운전을 목표로 건설 중이던 Chooze B 원전 (1450 MWe급 원전)에 적용코져 하였다. 그러나 초기에 구상하였던 계통설계내용이 너무 의욕적이고 복잡한데 비하여 개발 기간이 충분치 못하다는 점과 강화된 인허가 설계요건에 따른 소프트웨어 확인 및 검증이 불가능하다는 결론에 도달하여 1990년 12월에 프랑스 전력회사 (EdF)는 P20 개발계획 수정을 선언한 바 있다.

프랑스 원전의 계측제어계통 설계 개념은 안전성 측면에서 3등급 즉, 즉각적인 안전기능을 수행하기 위한 1E Class 설비, 장기적인 안전기능 수행에 필요한 2E Class 설비 및 이들 1E, 2E Class 설비를 지원하기 위한 IPS/NC 설비로 분류되는데 초기의 P20 개발 계획은 이들 모두를 Merlin-Gerin사에 발주하여 개발에 실패한 바 있다. 따라서 현재 EdF 사에서 추진중인 P20 개발 계획은 1E Class 계통 (SPIN)은 Merlin-Gerin 사에서 개발하고 2E Class 와 IPS /NC 계통 (Contronic E Process Control System)은 Hartman & Braun 사에 의해서 개발하는 것으로 알려져 있다. 그림 2에서는 Hartman & Braun 사에서 개발중인 Contronic E Process Control System의 개념도를 나타내었다.

이와 관련하여 프랑스 원자력 규제기관인 IPSN의 디지탈 계통설계에 대한 규제입장은 국제전기학회에서 제정한 소프트웨어 설계지침 IEC 880 Software for Computer in the Safety Systems of Nuclear Power Station 과 IPSN 에서 제정한 소프트웨어 품질보증지침 PAQS에 의거 설계된다면 허용가능한 것으로 알려져 있다. 따라서 불란서 원전 설계시 미국의 경우와 같이 디지탈 계통 채택에 따른 추가적인 사고해석이 요구되지 않는 것으로 알려져 있다.

3) 캐나다의 경우

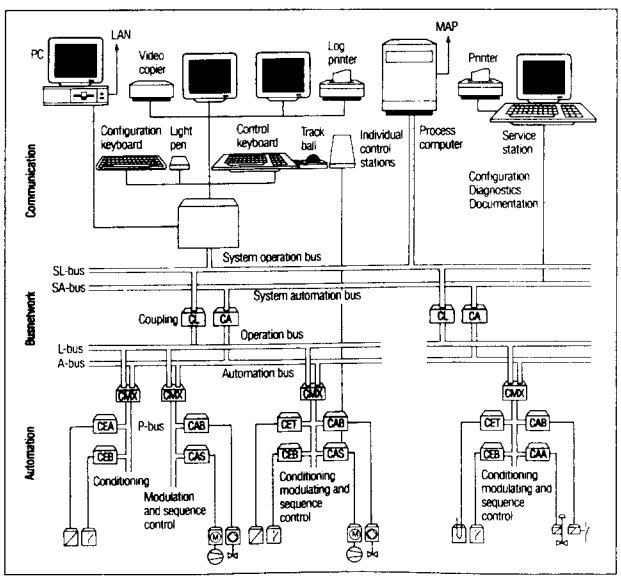


그림 2. Functional Structure of the Contronic E Process Control System.

CANDU 원전의 설계개념은 초기 모델부터 컴퓨터 제어 개념에 의한 계통설계를 추진하여 왔으나 안전기능을 수행하는 계통의 디지탈화는 1980년대 초기 CANDU 600 원전에 적용된 PDC (Programmable Digital Comparator)의 채택이 최초라 할 수 있다. PDC의 기능은 각종 원자로 운전변수를 감시하여 사전에 설정된 안전운전 제한치를 초과시 원자로 정지 및 각종 안전장치의 구동신호를 발생시키는 것으로 2개의 독립적인 원자로 정지계통 즉, SDS 1 과 SDS 2에 각각 설치되어 있다. 그림 3에서는 CANDU 600 SDS 1 PDC의 구성도를 나타내었다.

이 후 Ontario Hydro사에서는 원자로 정지계통 설계를 보다 개선하여 원자로 정지 기능 이외에도 자체 시험 및 고장 진단기능, 운전상태 지시기능 등을 보강하여 1990년대 초에 Darlington 원전에 설치하여 현재까지 운전중에 있다. 1970년대말 최초의 PDC 설계에 대한 인허가 심사가 진행될 당시 캐나다에는 안전관련 디지탈 설계에 대한 규제법규나 기술기준이 정립되어 있지 않았던 관계로 캐나다의 규제기관인 AECB에서는 PDC 계통의 운전신뢰성에 대한 사업자 분석 보고서 내용에 의거 설치허가를 발급한 바 있다. 그러나 이 후 원자로 안전계통의 설계는 다양성 설계(Diversity Design) 개념이 적용되어져야 한다는 점과 컴퓨터 소프트웨어의 공통모드고장(Common Mode Fail)을 방지하기 위한 설계과정중 품질보증활동이 강화되어야 한다는 내용의 새로운 규제요건을 제정하게 되었다. 이에 대하여 캐나다 최대의 전력회사인 Ontario Hydro 사와 AECL에서는 최근 안전관련 컴퓨터 소프트웨어의 개발지침 OASES(Ontario Hydro / AECL Software Engineering and Standard)를 개발하여 규제기관의 승인을 요청중에 있다.

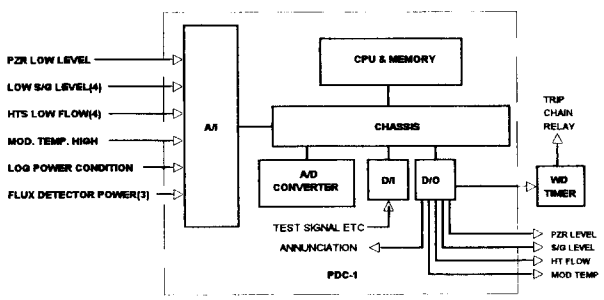


그림 3. CANDU 600 SDS 1 PDC Configuration.

4) 영국의 경우

원자력 발전소의 계통 설계시 디지탈 기술의 최초 적용은 1980년대 중반에 상업운전을 시작한 Heysham B_1&B_2 원전과 Dungeness B_1&B_2 원전이었다. 그러나 이들은 개스냉각 원자로(AGR) 방식으로 현재 세계적으로 주종을 이루는 가

압경수형 원전 계통설계시의 디지탈 기술적용은 최근 건설이 완료되어 상업운전을 시작한 Sizewell B 원전이 있다.

영국 원자력 산업계에서는 그동안 건설.운전 되어오던 개스냉각 방식의 원자력발전소를 지양하고 새로운 차세대형 원전의 모델로서 가압경수형 원전을 채택하였으며 Sizewell B 원전은 영국 최초의 가압경수형 원전이었다. 따라서 영국의 원자력 규제기관인 NII (Nuclear Installation Inspectorate) 에서는 1979년에 디지탈 계통설계에 대비한 안전성 평가 원칙 (SAP)을 제정한 바 있으며 이를 통하여 원전사고로 인한 방사선 대량누출 가능성은 10^{-7}/Reactor Year 이하로 유지할 것과 발전소 보호계통의 고장확률은 10^{-7} failure/demand 이하로 유지할 것을 가압경수형 원전의 규제기준으로 설정한 바 있다. 또한, 보호계통 구성은 중첩성 (Redundancy)과 다양성(Diversity) 원칙에 따라 설계하고 단일 찬넬의 고장확률은 10-4 failure/demand 이하로 설계할 것을 요구하였다.

이에따라 Sizewell B 원전 설계의 경우 디지탈 설계기술에 의한 Primary Protection System (PPS)과 기존의 Hardwired Laddic 설계기술에 의한 Secondary Protection System (SPS)를 병행 설치하여 필요시 각 계통이 독립적으로 원자로 정지와 필수안전 기능 수행이 이루어질 수 있도록 설계된 것이 특징이다. Sizewell B 원전의 PPS 계통은 Westinghouse 사에서 개발한 Eagle 21 IDPS을 이용하여 설계하였으며 소프트웨어는 PL/M-86 Language 사용하였다. 이 중 PPS 소프트웨어의 신뢰성과 안전성은 Sizewell B 원전의 인허가 심사 과정에서 가장 중요한 안전성 쟁점으로 부각되어진 바 있다.

한편, Sizewell B 원전의 소유주인 Nuclear Electric 사에서는 Westinghouse 사와 공동으로 PPS 소프트웨어의 신뢰성을 입증하기 위한 심층적인 설계평가 작업을 수행하였으며 그림 4에는 이러한 과정을 나타내었다. 그림 4의 내용 중 MALPAS는 PPS Source Code를 분석하기 위하여 사용되는 통계적 해석수단 (Static Analysis Tool)으로 세부내

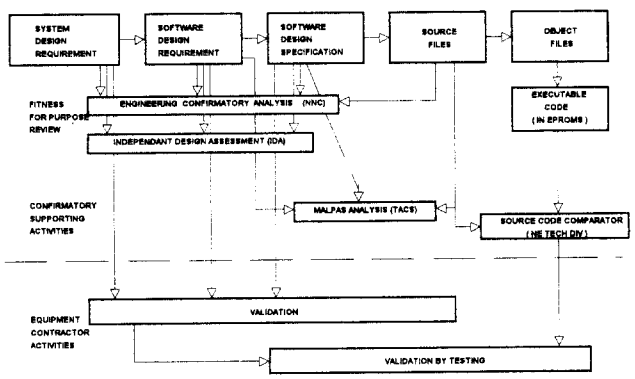


그림 4. Software Assessment Activities for Sizewell B Plant

용은 소프트웨어 프로그램의 구조와 데이터 의 전달과정을 분석하는 언어 구조해석 (Syntax Analysis) 과 입출력 신호간의 기능적 상관성을 분석하는 언어 의미해석 (Semantic Analysis) 이외에도 Source Code의 수식적 표현의 적합성을 분석하는 일치성 해석 (Compliance Analysis) 과정으로 분류 되어진다. 이러한 종합적인 분석과정을 통하여 Nuclear Electric사는 PPS 설계의 신뢰성을 입증하였으며 그 결과를 NII에 제출하여 Sizewell B 원전의 운전허가를 취득하였다.

5) 일본의 경우

세계 전자 산업계에서 선두 주자로 알려진 일본의 경우에도 원자력 발전소 설계에 디지탈 기술을 적용하는 문제는 매우 신중하고 보수적인 자세를 취하여 왔다. 그러나 1980년대 초반 원전 불시정지의 주요 원인이 노후화된 아나로그 계측제어 설비에 기인한다는 여론이 증대됨에 따라 당시 산업계에 보편화 되어 있던 전산화 계통(Microprossor-Based System) 설계를 원전 제어계통에 적용하기 위한 연구에 본격적으로 착수하게 되었다. 이에따라 일본 원자력 산업계에서 최초로 디지탈 제어계통의 적용된 원전은 1990년 상업운전을 개시한 Kashiwazaki -Kariwa 원전 2호기로서 이는 Ohi 2, 3호기 등과 같은 후속 원전의 설계에 디지탈 기술 적용영역을 점차 확대시키는 계기가 되었다. 또한, 최근 건설이 완공되어 상업운전을 준비중인 Kashiwazaki-Kariwa 원전 6, 7호기의 경우에는 발전소 제어기능 외에도 원자로 보호계통 설계를 디지탈화 함으로써 일본 원전 설계의 새로운 전환점이 되고 있다.

일본 원자력 규제행정을 담당하고 있는 통산산업부(MITI)에서도 이들의 기술개발 노력을 지원하고 원전설계의 안전성을 향상 시키기 위한 목적으로 관련 기술기준 즉, JEAG-4609 디지탈 계통설계의 품질보증기준과 JEAG-4101 디지탈 계통 설계의 확인 및 검증기준을 새로 제정한 바 있다. 그러나 현재까지도 일본 원자력 산업계와 일본 규제기관 간에는 디지탈 계통설계의 신뢰성 평가기준에 대한 이견이 조정되지 못한 상태이다.

3. 디지탈 계통설계의 안전성 심사

앞서 언급한 바와같이 디지탈 계통의 다양한 설계 장점에도 불구하고 원자력 안전관련 시설에 디지탈 기술을 적용하는 문제는 현재까지도 보편화 되어 있지 못한것이 현실이다. 이에대한 근본적인 원인은 현재의 기술 수준으로는 세계 각국의 원자력 규제기관에서 우려하고 있는 계통설계의 안전성에 대한 우려를 불식시키기 어려우며 원전 사업자의 입장에서 볼 때 새로운 계통설계의 확인 및 검증단계에서 소요되는 막대한 인력 투입으로 인한 경제성 저하 등이 장해 요인인 것으로서 알려져 있다. 표 1 에는 예로서 영국 Sizewell

표 1. Man-years of effort put into Sizewell B PPS.

Design by Westinghouse	200 man-years
V&V by Westinghouse	50 man-years
Design assessment by NE (PPG)	40 man-years
Engineering confirmation by NNC	40 man-years
Independent Design Assessment by NE (STB)	40 man-years
MALPAS confirmatory analysis by TACSL	80 man-years
Misc assessment by other parties	20 man-years
Dynamic testing by RR & A	15 man-years
Safety monitoring by NE (HSD)	15 man-years
Total	500 man-years

B 원전 보호계통 설계과정에 투입된 인력현황을 나타내었다.

표 1에 나타낸 바와 같이 디지탈 계통의 개발에 소요되는 인력 투입이 200 Man-year 인데 비하여 디지탈 계통의 설계평가 및 검증에 소요되는 인력 투입이 300 Man-year로 나타남으로 해서 원전 사업자의 입장에서 볼 때 디지탈 계통 설계에 대한 장해요인으로 인식 되어지고 있다. 그러나 이는 새로운 기술적용을 위한 과도기적 현상으로 향후 기술수준의 발전과 규제법규의 정비를 통하여 최소화 할 수 있을 것이다.

원자력 안전관련 시설의 디지탈 계통설계와 관련하여 제기되고 있는 주요 안전성 심사 현안은 다음과 같은 3가지 사항으로 요약 되어질 수 있다.

첫째, 디지탈 컴퓨터 계통 운전의 신뢰성을 어떻게 보증할 것이며, 특히 컴퓨터 소프트웨어 개발 단계에서 발생될 수 있는 프로그래밍 오류를 극소화 하기 위한 방안은 무엇인가?

둘째, 예상되는 모든 발전소 운전 조건 하에서 컴퓨터 하드웨어의 건전성을 보장하기 위한 검증 시험의 내용과 이에 대한 기술적 근거는 무엇인가?

셋째, 디지탈 컴퓨터 계통의 고장 또는 운전 오류 발생으로 인한 원자력 발전소 안전성 파급효과와 이에 대비한 심층방호 (Defense-In-Depth) 설계 대책은 무엇인가?

따라서 본 절에서는 이러한 문제에 대한 안전성 심사 현황을 살펴 보기로 한다.

1) 컴퓨터 소프트웨어의 신뢰성

컴퓨터 소프트웨어의 설계에 대한 안전심사 내용은 소프트웨어 개발과정에 대한 품질보증 활동과 설계 확인 및 검증 활동을 평가하는 것이다. 이러한 방법은 컴퓨터 소프트웨어의 개발과정에 대한 신뢰성을 평가하기 위한 것으로 컴퓨터 소프트웨어의 특성상 개발이 완료된 상태에서 제품의 신뢰도를 평가하는 것이 매우 어려운 것으로 인식되어지기 때문이다. 즉, 컴퓨터 계통의 신뢰도에 가장 주요한 영향을 미치는 인자는 컴퓨터 계통 운전용 소프트웨어 프로그램이며, 이는 기존의 아나로그 계통과는 달리 시험에 의한 방법으로는 신뢰도를 평가하는 것이 거의 불가능하다는 점이다. 따라서 미국의 원자력규제위원회(NRC)를 위시한 세계 각국 규제기관들은 컴퓨터 소프트웨어의 설계 및 설치단계에서 철저한 품질관리와 체계적인 자체평가가 이루어질것과 이에대한 내용이 문서화 됨으로서 추후 확인이 가능할 것을 원전 설계자에게 요구하고 있다.

이와 관련한 규제기준은 현재 IEEE Std 7-4.3.2-1993 와 IEEE Std 1012-1986, IEC Std 880-1986, ASME NQA-1-1989 등이 적용되고 있다. 이들 기술기준의 주요내용은 컴퓨터 소프트웨어의 신뢰성 증진을 위하여는 각 개발 단계에서 독립적인 설계 검토 조직에 의한 설계 검토 (Independent Reviews), 설계 참관(Independent Witness), 설계 검사(Inspection), 설계 분석(Analysis) 및 설계 시험 (Testing)이 수행 되어져야 하는 것으로 나타나 있다. 또한 이러한 설계 확인 및 검증 (V&V) 전 과정을 평가할 수 있는 검증 계획서(V&V Plan), 이상 결과 보고서(Anormaly Report), 최종보고서(V&V Final Report)의 작성내용을 규정하고 있다. 따라서 원전 규제기관의 역활은 이들 보고서 내용에 대한 평가를 통하여 설계 적합성을 확인하는 것이며 필요시 현장 방문 또는 사업자와의 회의를 통한 안전성 평가를 수행한다. 국내의 경우에도 영광 3, 4호기 운영허가 심사 과정에서 이와 같은 내용의 설계 안전성 평가가 한국원자력안전기술원에 의해 수행된 바 있다.

2) 컴퓨터 하드웨어의 성능검증

일반적으로 기존 원자력발전소의 아나로그계통 설계의 경우에도 안전관련 계통 또는 설비로 사용되기 위하여는 사전에 엄격한 성능검증 시험이 수행되어져 왔다. 원전기기의 성능검증 시험은 지진 발생으로 인한 진동 조건하에서 설비의 건전성을 보장하기 위한 내진검증(Seismic Qualification) 시험과 원자력발전소의 사고로 인한 극한 조건 하에서 설비의 건전성을 보장하기 위한 내환경 검증 (Environmental Qualification) 시험으로 분류 되어진다. 따라서 이러한 성능검증 시험요건은 디지탈 계통설계의 경우에도 동일하게 적용 되어진다. 이외에도 디지탈 설비의 경우에는 아나로그 설비에서 고려치 않았던 새로운 검증시험 즉, 전자계 간섭(Electromagnetic Interference : EMI)영향에 대한 대응능력(Electromagnetic Compatibility ;EMC) 시험이 추가적으로 수행되어져야 한다는 것이 원전 규제기관의 공통된 입장이다.

그러나 원전 디지탈 설비에 대한 EMC 시험내용과 범위는 현재까지도 수많은 논란의 대상이 되어오고 있다. 즉, EMI 현상은 디지탈 설비의 설치위치와 발전소 운영조건에 의한 영향이 주요 변수로 작용하므로 획일적인 시험기준을 적용하는 것은 문제가 있다는 것이 원전 사업자들의 주장이다. 현재 미국 NRC의 경우 EMC 시험요건은 Mil-Std-461C

Notice 2를 적용하고 EMI에 대비한 계통설계 및 설치요건은 IEEE Std 1050-1989와 IEEE Std 518-1982를 적용하는 것으로 규제방침을 확정한 바 있다. 국내 원전의 안전규제 업무를 담당하고 있는 한국원자력안전기술원(KINS)에서는 현재 국내에 건설 또는 운전중인 원전의 대부분이 미국형인 점을 감안하여 미국의 NRC와 동일한 규제입장을 취하고 있으나 향후 독자적인 규제기준 설정을 위한 연구를 진행중에 있다.

3) 심층방호 설계 개념의 적용

일반 산업시설의 경우와는 달리 원자력발전소의 설계과정에서 고려되어야 할 안전설계 사항의 하나는 심층방호 (Defense-In-Depth) 개념의 적용이라 할 수 있다. 즉, 심층방호 설계개념이란 비록 원전의 안전관련 계통이 매우 신뢰성 있게 설계되었다 하더라도 예상치 못한 고장 또는 비정상 작동에 대비하여 물리적 방호수단을 추가적으로 갖추도록 한 것으로 원자력발전소 보호계통의 기본설계 개념이다. 이와 관련하여 IEEE 7-4.3.2-1993 Appendix B 에서는 원전 보호계통의 구성을 이중화된 디지탈 컴퓨터 계통으로 할 경우 동일한 하드웨어와 소프트웨어를 사용시에는 가상사고 발생과 디지탈 컴퓨터 공동모드 고장을 고려한 사고해석(Defense-In-Depth Analysis)을 수행하고, 그 결과에 따라 다양성 설계(Diverse Design)를 채택할 것을 권고하고 있다. 이외에도 1993년에 발표된 미국 NRC 규제정책 보고서 SECY-93-087 에서도 원전 사업자는 해당 원전의 안전성 분석보고서(SAR)에서 다루어지고 있는 모든 사고 조건에 대하여 디지탈 계통의 공통모드 고장 발생을 가정한 사고해석을 수행할 것과 이때 발전소의 안전기능이 보장되지 않는다면 추가적인 발전소 보호수단(Diverse Function or Different Function)을 갖추도록 요구하고 있다. 따라서 원전 사업자의 입장에서 볼때 원자력발전소의 보호계통을 디지탈 계통으로 대체함으로서 추가적인 사고해석 (Defense-In-Depth Analysis)의 수행과 Diverse Backup 설비를 별도로 설치해야 하는 부담을 안게 되었다.

이러한 NRC 의 규제정책은 현재 세계 각국의 규제기관과 원자력 산업계의 안전성 쟁점으로 부각 되어져 있다. 즉, 영국과 일본 규제기관의 경우 NRC의 입장을 지지하고 있는데 비하여 프랑스와 캐나다 규제기관의 경우 추가적인 사고해석과 이에 따른 Diverse Backup의 설치는 불필요한 것으로 평가하고 단지 디지탈 계통의 공통모드 고장을 줄이기 위한 사업자 품질보증활동 강화를 유도하는 방향으로 규제법규를 재정비 한 바 있다. 국내 원자력 안전규제 전문기관인 한국원자력안전기술원에서도 현 단계에서는 NRC의 규제입장에 따라 추가적인 Hardwired Diverse Backup 설치를 원전 사업자에게 요구하고 있으나, 향후 디지탈 설계기술의 운전실적과 관련 분야 연구결과에 따라 규제요건을 재정비하는 것을 검토중에 있다.

4. 맺음말

본고에서는 최근들어 원자력발전소 설계에 적용범위가 급격히 증대되고 있는 디지탈 계측제어 계통의 개발현황과 안전규제 내용을 간략히 소개하였다. 디지탈 계측제어 계통의 신뢰성과 안전성에 대한 논란의 쟁점은 컴퓨터 시스템의 오동작 가능성과 이에 대비한 적절한 설계 보완 대책으로 요약될 수 있으며 이는 컴퓨터 소프트웨어의 공통모드 고장에 대한 우려로 귀착되어 질 수 있다. 따라서 원전 산업의 지속적인 발전과 원전 안정성에 대한 확고한 대중적 지지 기반을 구축하기 위하여는 컴퓨터 소프트웨어의 공통모드 고장 우려를 불식 시킬 수 있는 합리적인 방안이 강구 되어져야 할 것이다. 이를 위하여 세계 원전 산업계와 각국의 규제기관은 관련 연구와 규제법규 정비를 추진 중에 있으며 우리나라의 경우에도 이와 같은 연구개발 사업이 진행중에 있다. 현재 우리의 여건하에서 원자력발전소의 기술혁신과 안전성 향상은 동시에 추구 하여야 할 공동의 목표인 것이다.

참 고 자 료

[1] IEEE / ANS P-7.4.3.2, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, IEEE Power Eng. Society, 1993

[2] Digital Systems Reliability and Nuclear Safety Workshop, U.S. Nuclear Regulatory Conission, Sept, 13-14, 1993

[3] SECY-93-087, Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs, April 2, 1993

[4] F. Ridolfo et al., The Nuplex 80+ Advanced Control Complex from ABB Combustion Engineering, Nuclear Safety, Vol. 34. No 1, PP. 64-75, Jan-March 1993.

[5] Edgar M. Brown, Digital Safety System Operating Experience at ABB CE Plant, Nuclear Power Plant Journal, P.P. 25-29, May-June 1995

[6] James T. Keiper, Why Utilities Go Digital for I&C Replacement, Nuclear Engineering International, P. P. 34-36, November 1994

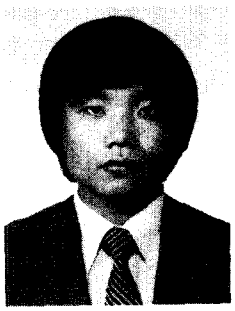
[7] B. Appell, Putting in a Replacement for Controlbloc P20 at Chooze B, Nuclear Engineering International, P.P. 45-47, July 1992

[8] Geoffrey Ives, Digital Systems Review of Safety

Critical Applications, Nuclear Engineering International, P.P. 37-40, April 1994.
[9] Sizewell B Reactor Protection Reliability : Nuclear Electric Presents Its Case, Nuclear Engineering International, P.P 28-34, March 1993

윤 원 영

저 자 소 개



윤 원 영

1952년 4월 6일생
1978년 인하대학교 전자공학과 졸업(학사)
1981년 인하대학교 전자공학과 졸업(석사)
1991년 한국과학기술원 원자력공학과 졸업(박사)
1978.~1984. 6 한국원자력연구소 전기전자공학실 선임연구원
1984.6~1985.12 프랑스 원자력연구소(CEN) 기술 훈련
1986~현재 한국원자력안전기술원 계측제어그룹장
305-338 대전광역시 유성구 구성동 19.
TEL. 042) 868-0237 / FAX. 042) 861-1700.