

고리1호기 디지털 발전소보호계통 설비개선에 대한 안전성평가

Safety Evaluation for digital upgrade of plant protection system in kori 1
nuclear power plant

고정수, 정충희, 오성현, 김복렬, 지성현

한국원자력안전기술원
대전광역시 유성구 구성동 19

요 약

국내 가동중 원전중에서는 최초로 고리1 호기 발전소보호계통설비가 디지털-기반 설비로 교체되었다. 동 설비개선의 주요 특징은 국내 업체의 주도하에서 안전계통에 사용되고 있는 아날로그 설비를 디지털-기반 설비로 교체한 점이다. 설계개선을 통하여 공정보호 및 제어 설비를 기존 Foxboro 사의 H-Line 모델(아날로그-기반 시스템)에서 SPEC 200 및 SPEC 200 Micro 모델(디지털-기반 시스템)로, 소내감시 설비를 웨스팅하우스사의 W-2500 시스템에서 우리기술(주)의 XM-7000으로 교체하였다. 본 설비개선과 관련한 운영변경허가 신청내용의 적합성 평가를 위해 계측제어, 인간공학, 전력계통, 안전해석, 기계설비 분야에서 안전성 검토가 수행되었으며, 디지털 시스템의 공통모드고장에 대비한 방어설계 적합성, 소프트웨어 확인/검증 방법, 전기적/물리적 독립성, 실시간 성능요건 및 기기검증 등의 규제현안사항들에 대한 중점적인 심사를 통하여 설비개선에 대한 안전성이 확인되었다. 본 논문에서는 이들 주요 현안사항들에 대한 검토방법, 검토결과를 기술하고 아울러 가동중 원전에서 디지털 설비개선공사에 대한 보다 효율적인 안전성 확인을 위해 필요한 사항을 제안하였다.

Abstract

The first replacement with digital-based I&C system in Kori unit 1 had been successfully applied to the process control, protection, and monitoring system. This Upgrade project started in Jan, 1998 and had been completed during its 17th over-haul in 1998. The upgraded system was implemented using the Foxboro Spec 200(analog module) and Foxboro Spec 200 Micro(digital processor) instrumentations instead of Foxboro H-Line. Safety Evaluation for the process protection and control system upgrade project of Kori Unit 1 was focused on the assessments for Digital System Functionality, Electrical/ Physical Separation, Quality Assurance of Software, DID & D Analysis and Equipment Qualification including EMI. This paper describes the scope of system upgrade, system functional description, technical approach to the evaluation, discussion, evaluation findings and conclusions. We have also provided the evaluation process considering lessons learned in evaluating this upgrade project to review effectively the safety of digital-based I&C system.

1. 서 론

고리1호기 공정보호 및 제어설비가 노후화 됨에 따라 대체품 확보의 어려움 등, 많은 문제점이 노출되었으며, 이러한 문제점을 해결하고 또한 신뢰성 확보 및 안전성 향상을 도모하기 위하여, 한전은 기존의 아날로그식 설비를 디지털-기반 계측제어 설비로 개선하기 위한 운영변경허가를 1998년 2월에 신청하였으며 1998년 9월에 현장설치 및 시험이 완료되었다. 동 설비개선 주요 특징은 국내 가동중 원전에서 최초로 안전계통에 사용되고 있는 아날로그 설비를 디지털-기반 설비로 교체된 점이며 설계 업무를 국내 업체에서 주도하여 후속 유사업무에 대비한 기술 자립이 추구된 점이다.

고리 1호기의 기존 공정보호 및 공정제어 계통은 H-Line 장비로 구성되어 있으며 이를 Foxboro사 SPEC 200 Micro 및 SPEC 200 입출력 모듈로 구성된 마이크로 프로세서 중심의 장비로 기능면에서 1:1 교체 내지는 최대 5:1의 비율로 집적화된 제어카드로 교체하는 것이 본 설비개선의 주요 내용이다. 교체된 공정보호 캐비닛들은 원자로보호계전기 캐비닛과 공학적안전설비계전기 캐비닛에 접점출력을 제공하고, 지시계, 기록계, 소내감시설비 컴퓨터, 제어계통 등에 격리된 아날로그 출력을 생성시키는 등 기존의 계통기능과 동일한 기능을 수행한다. 설계개선을 통하여 공정보호 및 제어 설비를 기존 Foxboro 사의 H-Line 모델(아날로그-기반 시스템)에서 SPEC 200 및 SPEC 200 Micro 모델(디지털-기반 시스템)로 교체하였으며, 소내감시 설비를 웨스팅하우스사의 W-2500 시스템에서 우리기술(주)의 XM-7000으로 교체하였다.

본 운영변경허가 신청 내용에 대한 적합성 평가를 위해 계측제어, 인간공학, 전력계통, 안전해석, 기계설비 분야에서 총 17명의 검토자가 안전성 심사를 수행하였으며, 본 운영변경허가 신청 내용에 대한 안전성심사는 디지털 시스템 기능현안에 대한 적합성, 전기적/물리적 독립성 설계 적합성, 소프트웨어 수명주기 품질보증 적합성, 공통모드고장에 대비한 방어설계의 적합성, 디지털 기기검증 적합성, 기기신뢰도 분석내용 적합성, 응답시간 및 설정치 분석내용 적합성, 전원공급설비 적합성 등과 같은 주요 현안들이 중점적으로 검토되었으며, 제작사의 소프트웨어 확인 및 검증문서 적합성 평가와 공장인수시험 입회감사 등을 통해 안전성을 확인하였다.

2. 설비개선 범위 및 내용

2.1 기능 및 구성

발전소보호계통은 그림 1에서 보는 바와 같이 현장전송기, 신호처리 캐비닛, 발전소 보호계통 캐비닛, 원자로정지계통 및 공학적안전설비작동계통 등으로 구성되어 있다. 공정보호계통은 신호처리 캐비닛에 설치되는 계통으로서, 현장 검출기(압력, 수위, 온도, 유량 등)의 신호를 입력받아 동 신호를 공정처리하고, 동 신호가 보호설정치를 초과하는 경우는 바이스태이블을 동작시켜 원자로정지 및 공학적안전설비 작동신호를 발생시키고 주제어반 지시계, 기록계 및 지시등을 통해 운전원에게 정보를 제공하는 계통이다. 본 계통은 채널 I, II, III, IV 등 4개의 그룹으로 분리되어 있으며, 현장 전송기를 통하여 입력된 신호 중 지시계 및 기록계와 연결되는 신호는 주제어반으로, 보호 및 안전 관련 신호는 원자로보호 및 공학적안전설비 계전기 캐비닛으로, 제어 관련 신호는 제어 캐비닛으로 신호를 공급한다.

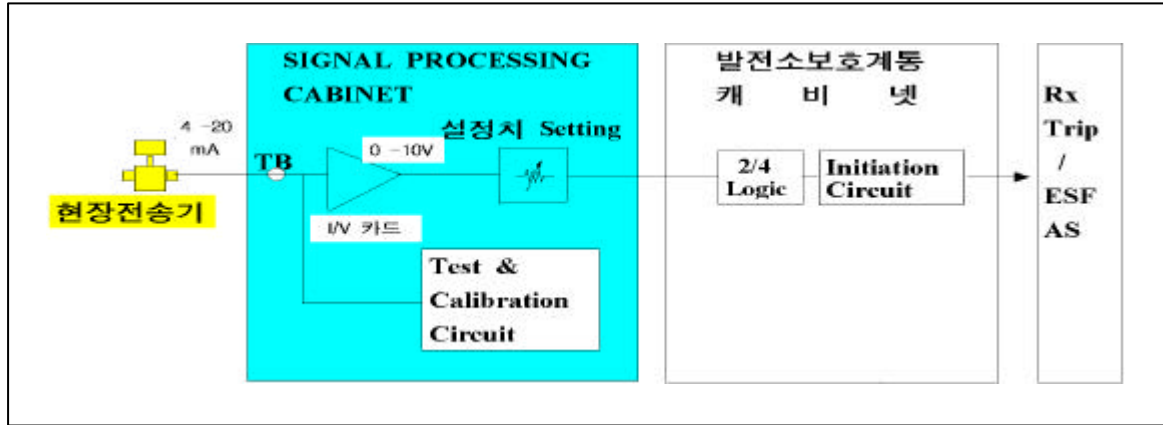


그림 1. 원자로보호계통 구성

2.2 설비개선 범위 및 내용

공정보호 및 제어설비계통의 개선범위 및 교체되는 제어모듈 수량등은 다음 표 1과 같다.

설비명	기 존 설 비	모듈수	신 규 설 비
공정보호 설비	H-Line (Foxboro사) - 12면 (Cabinet)	236	S200 + S200M (Foxboro사) - 8면 (4면 감소)
공정제어 설비	H-Line (Foxboro사) - 1차 : 10면, - 2차 : 13면(TBN Hall)	518	S200 + S200M (Foxboro사) - 1차 : 10면 (MCR) - 2차 : 6면 (MCR 집중화)
소내감시 설비	W-2500 (웨스팅하우스)		XM-7000 (우리기술(주))

표 1. 개선범위 및 교체제어모듈 수량

(1) 입력 모듈

입력신호 변환기 모듈(N-2AI-I2V)은 4~20 mA, 10~50 mA, 열전대, 저항온도계와 같은 아날로그 입력신호를 받아서 0~10 Vdc 신호준위로 변환시킨다.

(2) 프로세서 모듈

SPEC 200 MICRO 제어카드(N-2CCA-DF/SF)는 신호처리, 통제제어, 논리제어 기능을 수행하는 마이크로 프로세서기반의 카드로서 20개의 제어블록중 임의의 6개 제어블록을 선택하여 설계가 가능하다. SPEC 200 Micro 제어카드는 4 개의 아날로그 입력과 2 개의 아날로그 출력, 2 개의 접점입력과 2 개의 접점출력을 갖고 있다. 2 CCA 1대 당 최대 6개의 기능블록(Functional Block)를 처리할 수 있으며, 각 마이크로 제어카드는 자기진단 기능(Self-Diagnostic Function)을 갖추고 있다.

(3) 출력 모듈

제어 및 상태정보를 현장이나 다른 장치에 전송하기 위해서 4~20 mA 또는 0~10 Vdc 아날로그 신호처리 모듈과 계전기 스위치 모듈을 갖는 SPEC 200 출력변환기(N-2AO-V2I)가 제공되며, Class 1E와 non-Class 1E 신호 사이의 격리기 역할을 하는 모듈(N-2AO-VAI)이 있다.

2.3 설계내용 비교

공정보호설비계통의 주요변수에 대해서 설비교체에 따른 개선 전, 후 설계내용비교는 다음 표 2과 같다.

원자로정지 및 공학적 안전설비계통 공정보호설비					
번호	계 통	신 호 명	개 선 전	개 선 후	변 동 사 항
1	PZR Pr Channel	HI PR Rx Trip LO PR Rx Trip LO PR SI	Analog (H-Line)	Analog (Spec200)	아날로그
2	Cont't Pr Channel	Hi-1 Rx Trip Hi-2 Rx Trip Hi-3 Rx Trip	Analog (H-Line)	Analog (Spec200)	아날로그
3	S/G A&B Level Channel	Hi-Hi Rx Trip Lo-Lo Rx Trip	Analog (H-Line)	Analog (Spec200)	아날로그
4	PZR Level Channel	Hi LVL Rx Trip	Analog (H-Line)	Analog + Micro (Spec200+Spec200M)	아날로그/디지털 혼합형으로 변경
5	RCS Flow Channel	Lo Flow Rx Trip	Analog (H-Line)	Analog + Micro (Spec200+Spec200M)	아날로그/디지털 혼합형으로 변경
6	MS / FW Mismatch & MS Pr Channel	S/G LO LVL & LO Pr SI	Analog (H-Line)	Analog + Micro (Spec200+Spec200M)	아날로그/디지털 혼합형으로 변경
7	RCS Temp Channel	OT ΔT OP ΔT	Analog (H-Line)	Analog + Micro (Spec200+Spec200M)	아날로그/디지털 혼합형으로 변경

표 2. 공정보호설비계통의 주요변수에 대한 설계내용비교

3. 심사내용 및 결과

고리1호기 공정보호계통 설비개선과 같이 원자력발전소의 원자로 보호계통을 포함한 안전계통에 디지털기술을 이용한 컴퓨터-기반 계측제어계통을 채택할 경우 이에 대한 안전성 검토와 평가를 위한 접근방식은 기존 원전의 계측제어설비에 적용된 규제요건 외에도 디지털기술에 관한 규제지침들을 추가로 적용해서 신청된 디지털계통을 검토하고 평가하게 된다[1].

아날로그 계측제어계통으로부터 디지털 계측제어계통으로 바뀌는 주된 요인은 필요한 아날로그 재고품을 충분히 지원하지 못하는 것도 중요한 요인이지만 기존 아날로그 계통에 비해서 디지털 계통이 일부 장점들을 갖고 있기 때문이다. 예를 들면, 디지털 전자장치는 아날로그장치에 비해서 표류(Drift) 현상이 거의 없어서 검교정 결과가 훨씬 우수하고, 정확도와 계산능력의 향상으로 계통 성능이 향상될 수 있다는 점이다. 또한, 디지털계통은 설계가 잘 되면, 사용이 용이하고 훨씬 융통적이며, 또한 요구된 신뢰도를 달성하기 위해 새로운 개선 능력, 즉 고장허용기법, 자기-시험능력, 신호검증기법, 진단기능 등을 가질 수 있다. 한편, 디지털 계측제어계통을 원자력 발전소에 성공적으로 채택하기 위해서는 안전성 확보를 위한 규제관점에서 몇 가지 기술적인 현안사항들이 있으며, 고리 1호기 공정보호계통 설비개선에 대한 안전성 확인과정을 통하여 디지

탈 계측제어계통에 대한 이들 기술적 규제현안들이 적절히 해결되었는지를 중점적으로 검토하였다. 변경되는 디지털 계측제어계통은 가압경수로형 안전심사지침(NUREG-0800)은 물론, 기존의 인허가 규제요건, 즉 10 CFR 50.55a(h), IEEE Std 279, 603, 10 CFR 50, App. A(일반설계기준)와 App. B 등을 만족해야 하며, 특히 변경된 계통이 미 변경된 부분에 영향을 주지 않아야 한다. 아울러, 디지털계통이 10CFR50의 기본적인 허용기준을 따르고 있는지를 평가함에 있어서 아날로그계통에 비해 특별히 고려해야 할 사항들로서는 전자파 적합성(EMC)을 비롯한 환경검증, 소프트웨어의 품질보증내용, 심층방어 및 다양성평가, 실시간 결정론적 성능 보장, 온라인 시험 및 주기시험 설비, 그리고 독립성 등이 있으며 이들 기술적 현안사항들에 대한 평가결과는 다음과 같다.

3.1 적용기술 기준의 적합성

기존 계측제어계통에 적용되는 설계기준 외에 디지털계통에 추가적으로 요구되는 기술기준에의 적합성을 검토한 결과 IEEE 603에서 요구하고 있는 “단일고장기준”, “품질”, “고장시 안전모드로 작동”, “시험 및 교정능력”, “정보지시” 및 “출입관리”등의 설계요건들을 만족하도록 설계한 것으로 확인하였다. 또한, 마이크로 프로세서를 기반으로 하는 SPEC 200 Micro카드의 소프트웨어 설계는 R.G. 1,152에서 인증한 ANSI/IEEE 7-4.3.2요건에 따라 개발한 것으로 확인하였다. 한편, 사고후 감시계측설비의 설계 적합성과 관련하여 최종안전성분석보고서(FSAR) 7.5절에서 명시하고 있는 Condition II, III, IV 사고시 운전원의 수동조치에 필요한 계측설비중 Reg. Guide 1.97의 분류기준에 따른 Category 1 변수에 대해서는 Class 1E 요건(독립성)을 만족하여야 되나 이와 같은 요건을 만족하지 못하는 일부 변수가 확인되었으며, 해당 변수들에 대해서는 원자로 보호계통 캐비닛(NPS)에서 직접 주제어실의 지시계로 신호가 전달되도록 설비개선을 하도록 하였다.

3.2 실시간 성능요건의 적합성

디지털컴퓨터 기반 설계특성을 고려할 때, 타이밍 요건, 구조, 설계이행내용은 확인되어야 하며, 이를 위해서 설계기준사고로부터 계산된 시스템 타이밍 요건이 디지털 컴퓨터계통부분에 적절히 할당되었는지, 또한 디지털 시스템 구조설계에서 그 기준이 만족되었는지를 확인하여야 한다. 설계기준 서류들은 계통타이밍 요건을 기술해야 하며, 타이밍 요건들은 설계이행 과정을 통해 만족되어야 한다. SPEC 200 Micro 제어모듈의 구조는 제어 블록의 주기적인 처리실행방식으로 구현되며, 제어주기는 200 millisecond로 설정되어 있다. 처리 시간과 관련한 주요 기능을 확인한 결과, 각 제어 주기동안 연속적으로 마이크로프로세서에 의해 수행되는데 먼저, 입출력 하드웨어로부터 오는 입력이 프로세서 RAM에 복사되고, 두 번째로 6개까지의 제어 블록 각각이 처리되며, 세 번째로 제어 블록에 의해 계산된 결과는 프로세서 RAM으로부터 I/O 출력 하드웨어로 복사된다. 네 번째로는 200 millisecond의 나머지 시간이 화면을 갱신하고 낮은 우선 순위 태스크를 처리하기 위하여 사용된다. 처리 과정을 간략하게 요약하여 기술하면 그림 2와 같다 [2].

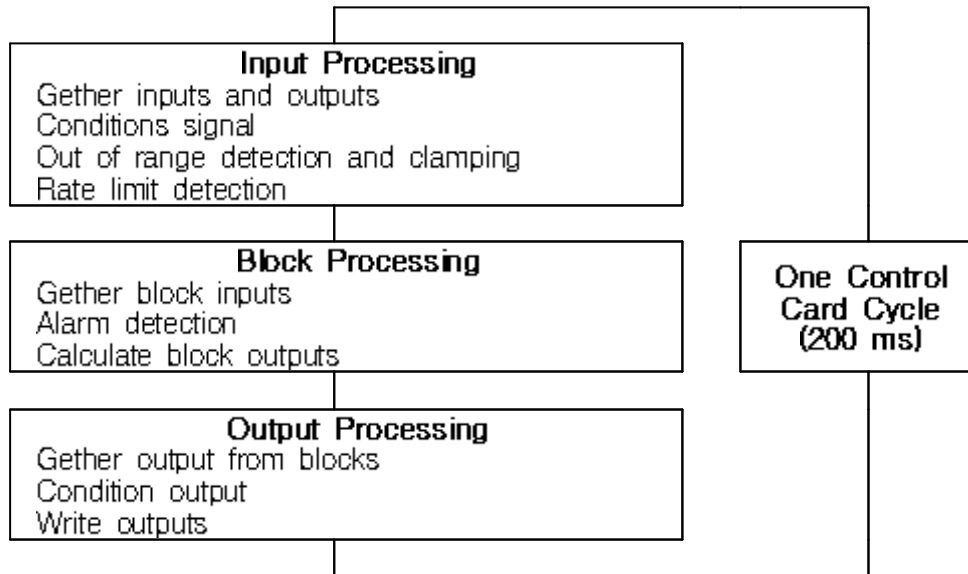


그림 2. SPEC 200 Micro 제어카드 내의 입, 출력처리 알고리즘 개략도

한편, 시스템 타이밍 요건명세내용이 공장인수시험과정을 통하여 확인되는지를 확인한 결과, 응답시간시험절차서[4]를 통해 수행됨을 확인하였다. 아울러, 디지털 시스템 타이밍 설계의 설계 이행사항 및 성능검증을 통한 적합성을 확인한 결과, Foxboro Spec 200의 최대 응답 시간 계산을 계산하여 발전소 기술지침서에 만족함을 보여줌으로써 실시간 성능의 적합성을 입증하였으므로 적절한 것으로 평가되었다.

3.3 가동중 시험 (on-line) 및 주기 시험 적합성

시험과 교정에 대한 설계내용을 검토한 결과, 공정보호계통(NPS)에 대한 정기시험은 매월 계열별로 수행하고 교체되는 Spec200/200Micro도 기존 H-Line과 동일한 시험기능을 확보하도록 설계되어 있으며, 각 공정변수들에 대하여 시험기간 동안 “출력운전중 시험”을 할 수 있도록 하기 위하여 바이스테이블의 출력을 수동으로 트립모드로 전환하도록 절차서에 명기되어 운영하고 있음을 확인하였다.

공정보호계통캐비닛의 시험패널 설계에는 SPEC 200으로 입력모듈을 구성한 아날로그회로 부분 및 SPEC 200 MICRO로서 프로세서부분을 구성한 디지털회로 부분을 모두 포함하여 상온정지에서 전출력 운전까지 주기적인 시험이 이루어 질 수 있도록 설계되어 있으며, 기술지침서에서 요구되는 채널시험수행을 위하여, 측정변수와 같은 모의 입력신호(공정변수)를 계측채널에 개별적으로 가능한 한 센서와 가까운 곳에 모의신호를 주입하여, 바이스테이블 트립이 적절하게 출력될 수 있는지를 확인하기 위한 시험용 잭이 시험 패널상에 각 공정채널로 설계되고, 시험입력을 정확히 측정하고 상호 연관시킬 수 있도록 시험점들이 설계되었음을 확인하였다.

한편, 디지털 컴퓨터를 근간으로 한 계측 및 제어계통은 기존의 아날로그 계통과는 다른 종류의 고장이 발생할 수 있다는 점을 고려하여 디지털컴퓨터 기반의 계측 및 제어계통을 초기화 할 때 컴퓨터계통 작동을 검증하기 위해 지속적인 자기시험 특성을 갖추어야 한다. 전형적인 자기시험은 감시 타이머 혹은 프로세서(중앙연산처리장치)를 이용한 기억장치의 건전성 감시, 그리고

중앙연산처리장치 상태의 감시, 자료의 건전성 감시가 포함될 수 있다. 이에 대한 설계내용을 검토한 결과, 자기진단에 의하여 감지된 고장은 즉각 주제어실 운전원에게 경보를 제공하여 수동적인 조치가 이루어지도록 되어 있음을 확인하였다. Foxboro사의 SPEC 200 MICRO 시스템은 전원 인가시, 제어모드로 전환시, 제어모드시 및 Standby 모드시 등의 모든 운전모드에 대하여 자기진단기능 시험이 수행되고 있고, 이 때 메모리와 입출력 등의 모든 하드웨어 및 관련된 소프트웨어들이 시험되도록 설계되어 있음을 확인하였다. 또한, '98.4.27일부터 '98.5.1까지 미국 Foxboro사에서 현장감사를 통해 SPEC200Micro 제어카드 개발당시의 품질보증서류를 확인한 결과, 자기진단(Self-Test) 기능이 초기단계인 요건명세단계에서부터 설계되고 시험되어 있음을 확인하였다. 즉 문제점 감지시 고장진단시험을 수행하며 오동작 감지 및 관련 데이터 제거기능 및 경보발생기능 등이 설계되어 있는 것으로 확인되었으며 자기진단시험의 종류로서는 전원 인가시 온라인 고장진단시험, 제어모드로 전환시 고장진단시험 및 Standby 모드시 고장진단시험 등으로 구별되며 주요 진단내용으로서는 ROM에 대한 Checksum 수행, RAM에 대한 패리티 체크 수행 및 Watch-Dog Timer의 작동 등으로 설계되어 있음을 확인하였다.

3.4 독립성 설계 적합성

안전계통 회로와 비안전계통 회로 신호간의 전기적 독립성을 만족하기 위하여 사용되는 격리기가 Class 1E 품질등급 요건을 만족하는가를 검토한 결과, 격리기로 사용된 전압/전류 변환기(Model No. N-2AO-VAI)는 요구되는 다음과 같은 기능시험내용을 만족하고 있음을 확인하였으며, 격리기의 출력측인 비안전급 회로에서 발생가능한 고장(회로의 단락, 개방 등)이 있더라도 안전급 회로의 성능이 허용수준 이하로 저하되지 않을 것으로 판단되었다. 즉, 전력선과 신호선에 가해질 수 있는 과전압/과전류(고장전압 또는 전류)의 시험전압은 대상설비에 가해질 수 있는 최대회로전압(실제 회로전압 120V AC)으로서 600V 교류전압을 인가하여 내성시험을 수행하였으며, 120Hz, 2.5KV의 공통모드 써지(Surge), 1.25KV의 정상모드 써지를 전원선에 2초 동안 가하여 신호변환기의 출력신호 변화가 스펠의 0.1%이하, 릴레이 모듈의 트립(오동작)이 없이 수행되었음을 확인하였다. 또한, 과도잡음(EFT/B)을 전원 및 신호선(RTD 신호선 제외)과 보호접지 사이에 가하여 시험을 수행한 결과도 관련요건을 만족한 것으로 평가하였으며, 정전기방전시험이 IEC Pub. 801-2의 요건에 따라 수평 및 수직 접지평면에 인가하여 모듈, 카드의 기능을 시험하였으며, 캐비닛의 외부표면에 $\pm 6KV$ 의 정전위 방전을 10초 간격, 10회 방전시켜서 기능을 확인한 시험결과도 허용기준을 만족하였음을 확인하였다. 한편, 운전과정에서의 안전성 확보를 위하여 공정보호 캐비닛 문을 개방할 때에는 항상 운전원이 정전기 써지 보호용 접지대(wrist strap)를 착용하도록 하는 제한조건을 Spec. 200/SPEC. 200 micro 설비의 운전, 점검(보수) 절차서에 명시하도록 요구하였다.

한편, 물리적 독립성 설계 적합성을 평가한 결과, 교체되는 설비는 분리독립된 기존의 필수 교류전원으로부터 전력을 공급받는 각각 독립된 4개의 캐비닛에 설치되므로 기기 및 전원공급계통에 요구되는 물리적 독립성 설계요건을 만족하고 있는 것으로 평가하였으며, 일부 사고후감시 계측설비에 대해서는 적절한 설계보완을 요구하였다.

3.5 소프트웨어 수명주기 공정계획, 이행, 결과물의 적합성[5]

소프트웨어 확인 및 검증문서의 적합성을 평가하기 위하여 미국 Foxboro사에서 제작사에 대한 현장감사를 통해 표준제어 블록 알고리즘을 포함하는 2CCA 카드 ROM의 버전-13 운영체통용 소프트웨어와 고리 1호기 제어기능을 수행하는 응용소프트웨어에 대한 개발과정에서의 품질보증내용을 관련기술기준인 IEEE-7-4.3.2를 기준으로 적합성을 확인한 결과, IEEE-1024에서 정의하고 있는 소프트웨어의 수명주기에 따라 구분하여 개발되었고 각 단계별 공정내용이 공동제품 사양서(CPS), 상세기능 사양서(DFS), 소프트웨어설계 사양서(SFS), 프로그램 기술 사양서(PTS) 및 마스터안내서(MI) 등의 문서에 대한 검토를 통해 적합한 것으로 평가하였다. 다만 소프트웨어 확인 및 검증시험절차서 및 시험결과보고서 내용을 확인한 결과 자기진단기능에 대한 성능확인 시험절차서가 일부 애매 모호하게 작성되어 시험이 수행되어 있으며 이는 관련 규제요건인 IEEE-7-4.3.2의 5절(통합시험) 및 6절(컴퓨터계통 검증시험)을 만족하지 못한 것으로 판단하여 보완하도록 요구하였으며, 재 실시된 자기진단기능 성능확인시험결과를 검토한 결과, 재시험이 적절히 수행되었음을 확인하였다. 또한, SPEC 200 Micro 제어카드는 공정제어기능 처리시 시간과 날짜를 이용하지 않는다는 설계내용 확인을 통하여 Y2K 문제가 없는 것으로 평가하였다.

3.6 공통모드고장에 대비한 방어설계의 적합성

디지털 설비개선과 관련된 심층방어 및 다양성 분석은 NUREG/CR-6303에 제시된 방법에 따라 정성적으로 이루어졌으며, 이와 같은 방법은 대체적으로 관련된 규제지침 및 입장을 반영한 것으로 평가되었다. 다양성 및 심층방어 분석에서는 최종안전성분석보고서 15장의 3가지 조건사건, 즉 (1) RCS 부주의한 감압사건을 포함한 13가지의 조건 II 사건(빈번한 주기의 결함), (2) RCS 강제유량의 완전상실사건을 포함한 5가지의 조건 III 사건(희박한 주기의 사건), 그리고 (3) 냉각재 상실사고를 포함한 7가지의 조건 IV 사건(제한적인 결함) 각각에 대해서 정성적인 평가 방법으로 분석이 이루어졌는데 동 분석에서는 먼저 원자로 보호시스템의 구성 기기와 모듈을 작은 기능별 단위인 "블록"으로 분해하고 블록 내에서 발생한 고장은 그 블록의 모든 출력신호를 훼손시키므로 하부의 블록들에게 고장이 파급된다고 가정하는 방법으로 안전성분석보고서의 15장에 있는 모든 사건들에 대하여 공통모드고장을 함께 가정하고 다양성 및 심층방어 분석이 수행되었다[6]. 분석결과에서 다중성 채널들에 대한 공통모드고장 취약점(6건)과 전체 공통모드고장 취약점(5건)이 확인되었고, 이와 같이 공통모드고장에 취약한 것으로 확인된 사건과 기능들에 대해서는 대체수단으로서 관련 트립변수들인 가압기 압력, 증기발생기 수위 그리고 격납건물 압력 채널들을 SPEC 200 Micro 모듈 대신에 SPEC 200 아날로그 모듈로 구현하였으며, 동 설계내용은 공통유형고장을 방지할 수 있는 설계로 평가하였다.

한편, 다양한 보호기능을 필요로 하는 사건들 중에서 최소한의 두 방어계층 요건을 만족하지 못한 사건 "통제불능의 보론 희석"의 경우에는 유일한 자동 트립변수가 OT/TT인데 이 변수 모듈이 공통모드고장으로 인해 상실되면 신호의 다양성을 잃게 되지만, 보론 희석으로 인한 반응도 주입이 매우 완만하고 동 사건의 거동을 감지 및 지시할 수 있는 정보설비가 운전원에게 충분히 마련되어 있고, 또한 운전원이 그것을 보고 판단하여 적절한 조치를 취할 수 있는 충분한 시간(약 30분)이 허용되어 있는 것으로 판단하여, 운전원의 수동조치만으로도 적절한 대체수단으로 유효한 것으로 평가하였다. "주급수시스템의 고장으로 인한 과다한 열제거"의 경우 원자로 트립변수는 OT/TT와 OP/TT가 있으며, 이 변수들은 동일한 디지털 모듈들을 공유하고 있으므로 동 모

들에서 공통모드고장이 발생할 경우 신호의 다양성을 잃게 되고, 직접적인 원자로 트립기능이 상실되지만 증기발생기 수위채널을 아날로그 방식으로 그대로 유지함으로써 증기발생기 고-고 수위에 의한 터빈 트립이 발생할 수 있고, 계속해서 터빈 트립에 의한 원자로 트립기능이 이루어질 수 있는 것으로 평가하였다. 이것은 기능적 다양성을 유지하고는 있지만 직접적인 트립경로가 상실되는 약점도 있으므로 안전성 향상을 도모하기 위하여 10CFR 50.62에 따른 ATWS 완화설비를 설치하는 방안을 강구하도록 요구하였다.

3.7 전자기파 기기검증 적합성

내전자기파 시험에서는 전자기파 방사(Emission) 시험 5가지(CE101, CE102, CE103, RE101, RE102)와 감응도(Susceptibility) 시험 7가지(CS101, CS114, RS101, RS102, RS103, IEC801-4, IEC801-5)가 수행되었으며 3가지 시험(RS 103, CS114, IEC801-4)을 제외하고는 관련요건을 만족하는 것으로 평가되었다[7]. 1차 Wyle Lab.에서 실패한 3가지 시험, 즉 RS 103(연속 고주파 방사감응 전계 시험), CS114(전원 및 신호선 전도 감응시험) 및 IEC801-4(전원선 및 신호선의 EFT/B 시험) 시험에 대해서는 재시험이 수행되었으며 재시험 결과, RS 103과 CS114 시험은 적합한 것으로 확인되었으나, IEC801-4 시험에서 일부 문제점이 확인되었다. 즉, IEC801-4 시험에서 전원선과 대부분의 신호선은 시험기준을 만족하였으나 RTD 신호선이 EPRI 기준을 만족하지는 못하고 허용기준이 다소 완화된 IEC의 LEVEL 2 기준을 만족하였다. 동 사항에 대해서는 고리1호기 보호시스템의 설치장소가 제어실이라는 점과 기기, 비차폐전원선 및 신호선 등이 채널별로 분리되어 설치되어 있으며, 제어실의 보호시스템 캐비닛에 연결되는 케이블이 설치된 주변에 고전압전선이 인접하여 설치되지 않는 점등을 고려하여 IEC 801-4 Level 2 기준적용이 타당한 것으로 평가하였으며, 실제 캐비닛 주변의 대형 전동기의 기동, 정지 등 고주파 잡음을 모의한 조건에서 잡음강도가 IEC801-4의 Level 2 시험기준인 $\pm 0.5\text{kv}$ 이내임을 확인하였으므로 적합한 것으로 평가하였다.

3.8 설정치 분석내용 적합성

원자로정지 및 공학적안전설비 관련 공정채널에 대한 기기오차, 트립설정치 및 허용치 계산을 ISA-S67.04에 따라 수행한 방법론은 적합한 것으로 평가하였으며, 공정신호처리 캐비닛에 포함되어 있는 입력신호처리 모듈의 불확실성 인자중 드리프트 요인이 39일에 대해 분석된 사항에 대해서는 고리 1호기 입력신호처리에 대한 교정시험 주기가 18개월로 이루어지고 있는 점을 감안하여 입력신호처리 모듈의 드리프트에 의한 불확실성 인자를 18개월에 대해서 평가하여 보호시스템의 설정치분석을 재 수행하도록 요구하였다. 사업자는 이에 따라 보호시스템 설정치분석을 재 분석하였으며 그 결과는 적절한 것으로 평가되었다. 또한, 상기한 설정치 재분석결과 도출된 설정치 변경내용이 최종안전성분석보고서 16장 및 운영기술지침서에 반영되도록 요구하였으며, 최종안전성분석보고서 16장 및 운영기술지침서의 보호시스템 트립 설정치 및 허용치가 적절히 개정되었음을 확인하였다[8]. 따라서 본 설정치 재분석에 따른 후속조치 내용은 타당한 것으로 평가하였다.

3.9 공장인수시험의 적합성

공장인수시험 절차서가 전 채널에 대해 렉 구성 및 점퍼세팅을 점검한 후, 아날로그 모듈의 입출력 기능, 마이크로프로세서의 공정처리 기능, Lead/Lag 소자의 동적응답 등과 같은 기능시험을 실시하고, 전원상실 또는 도어 개방과 같은 고장모드를 확인점검하도록 작성되어 있어 전반적으로 적절히 작성된 것으로 평가되었으나, 일부 설정치(3건)는 FSAR과 불일치하였으며, 입출력 모듈 교정시의 온습도 조건이 고려되지 않았고, Configurator의 기동모드에 대한 성능확인시험이 누락되어 있어 현장 감사 기간중 이를 절차서에 포함시켜 시험하도록 요구하여 이에 따라 시험이 실시되었다.

한편, 상기 사항 외에 "RTD 저항-온도 특성곡선"이 부적합한 것으로 확인된 내용은 즉각적인 보완이 불가능하여 현장인수시험(SAT) 절차서 작성시 RTD 제작사인 MHI사의 특성곡선을 반영하여 관련 시험을 실시하도록 요구하였으며, 동 사항은 현장 시험시 적합하게 반영되어 시험이 적절히 수행되었음을 확인하였다. 공장인수시험에 대한 현장 감사를 통하여 공장인수시험 및 시간응답시간이 절차서에 따라 적절히 수행되었으며, 공정보호채널 구성 점검, 채널기능시험, 고장모드 확인점검, 아날로그 모듈의 입출력 교정, 마이크로프로세서 모듈의 예상 출력, Lead/Lag 소자의 동적응답, 각 보호변수별 시간응답시험 등과 같은 점검 및 시험 결과가 판정기준을 만족하고 있는 것으로 확인하였다. 공장인수시험에 대한 현장 감사과정에서는, 시간응답시험 절차서에 허용기준 미수립 및 기술지침서에서 요구하는 응답시험 측정항목들의 다수 누락(8건)등 보완 사항들이 확인되었으며, 또한 Lead/Lag Term이 포함된 시험의 경우 시험방법이 미흡한 것으로 판단되어 이를 보완하여 절차서를 재작성하도록 요구하였다. 이를 보완하여 재작성된 절차서를 검토한 결과 OP Δ T, OT Δ T 시간응답시험의 경우 "입력 Case 선정의 부적합", "시험변수 입력 변화폭의 기준 불만족", "f(Δ Q) 기울기의 FSAR 변경내용 미고려" 등과 같은 추가 보완사항이 확인되었으며 이들 사항들에 대한 보완이 현장인수시험(SAT) 절차서에 적절히 반영되었는지 확인한 결과, 적절히 시정조치되었음을 확인하였다[3].

4. 결론

고리 1호기 공정보호 및 제어설비의 설비개선과 관련하여 제출된 최종안전성분석보고서 개정 내용과 안전성분석보고서 내용에 대하여 디지털 시스템의 공통모드고장에 대비한 방어설계 적합성, 소프트웨어 확인 및 검증 방법, 전기적/물리적 독립성, 실시간 성능요건 및 기기검증(EMI 포함) 등의 현안사항들을 중심으로 검토를 수행한 결과 전반적으로 디지털 설비개선과 관련된 규제요건과 제반 기술기준을 충족시키고 있는 것으로 평가하였다. 검토과정중 도출된 사고후 감시 계측설비 신호전달경로의 개선 및 ATWS 사고완화용 다양성 보호설비 설치등 보완사항들에 대해서는 적절한 시정조치가 진행중에 있으므로 본 공정보호 및 제어설비 개선공사는 적절히 수행된 것으로 평가하였다.

이번 설비개선공사에 대한 안전성 확인과정을 통해 얻은 교훈으로서, 앞으로 예상되는 가동중 원전에서의 디지털 설비개선공사를 보다 효율적으로 수행하기 위해서는 첫째, 사용자와 설계자의 상호 긴밀한 연계체제를 구축하게 할 수 있는 사업관리계획의 작성이 필요한 것으로 사료되며 둘째, 충분한 안전성 검토기간이 확보될 수 있도록 제도적인 장치가 마련될 것을 제안한다.

참고문헌

- [1] KINS-G-001, 경수로형 원전 안전심사지침서,
- [2] 고리 1호기 공정보호계통 설비개선 안전성분석보고서
- [3] KINS/AR-562, 고리 1호기 공정제어 및 보호설비 개선공사에 따른 운영변경허가
심사보고서, 한국원자력안전기술원, 1998, 6
- [4] 97F53252-TR-1002, "Module And Loop Response Time Analysis"
- [5] 97F53252-TR-1007, "Conformance Of SPEC 200 MICRO To Criteria For Digital
Computers Used In Safety Systems Of Nuclear Power Generating Stations"
- [6] 1-700-J406-001, "Diversity And Defense In Depth Analysis Forkori Nuclear Power Plant
Unit 1"
- [7] 46615-02, "EMI Test Report On a S200/S200M Control System"
- [8] 1-700-J351-002, "Instrument Uncertainty And Setpoint Calculation For Kori Nuclear
Power Plant Unit 1"