원자로 보호 계통 설계 개선
-Design Improvement on Reactor Shutdown System in Nuclear Power Plant-

박 철 주 *
Park,Chul-Joo
김 석 남 **
Kim.Suck-Nam
오 연 우 ***
Oh,Yon-Woo

Abstract

The special safety systems are incorporated into the plant design to limit radioactive releases to the public in the event of an accident. Wolsung 2 is better builted than Wolsung 1 by 84 design changes for new approval requirements, codes & standards changes and manufacturing changes etc. This paper analysed and discussed the design change items for nuclear reactor safety system and needs development of design engineering for digital protection system.

1. 서 론

원자로 설비는 모든 가상 사고에 대비하여 특수한 공학적 안전 설비를 갖추고 있어 각종 재해 및 인위적 사고에도 신속하고 안전하게 원자로를 정지시키도록 설계되어 있고 이러한 목적으로 설치된 4종의 특수 안전 계통은 상호 독립적으로 작용하여 천재 지변, 내외부 비행물체 등에 의한 충격에도 원자로의 안전성을 보장하며, 사보타지 등과 같은 인위적 가해에도 사고가 확대될 수 없도록 설계되었다. 비록 심각한 사고에 의해 방사능이 유출되는 경우에도 이를 원자로 건물 내에 수용하여 공중에 대한 방사능 피해를 방지하도록 보장하고 있다.

월성 2호기는 새로운 인허가 요건 변경, 적용 코드 및 기준(Code & Standard) 변경 및 요건강화, 생산 및 제작 중단에 의한 변경 그리고 기타 변경 요구에 의해 총 84개의 설계 변경을 적용하여 1호기 보다 진보, 개량된 발전소로 설계, 건설 중에 있으며, 원자로 보호 계통과 관련한 주요 설계 변경(DC ; Design Change)항목은 다음과 같다.

---

* 한국원자력연구소, 핵연료품질관리분야
** 한국원자력연구소,제어계통분야
*** 한국원자력연구소,품질평가실

2. 월성 2호기 원자로 보호 계통

2.1 설계 개념

. 구성품 고장시 안전한 방향으로 동작(Fail Safe)
. 다중화(Redundancy)
. 다양화(Diversity)
. 물리적 상호 격리(Physical Separation)
. 내진 및 내환경 검증 설계(Seismic & Environmental Qualification)
. 시험 능력(Testability)

2.2 보호 계통의 안전 설계 현황

2.2.1 발전소 주제어실은 물론 예비 제어실(SCA)에서도 원자로를 안전하고 신속하게 정지시킬 수 있도록 설계됨.

2.2.2 그룹별 설치 위치 분리

2개 그룹에 속한 계통의 기기 설치 위치는 원자로 건물 주위에서 90도 이상의 거리에 설치됨.

2.2.3 채널의 다중화

계통별 트립 채널을 3개로 구분하고 이중 2개 이상의 채널로부터 트립 신호 발생시 안전 계통이 동작됨.

2.2.4 채널 설비간 최소 이격 거리 확보

최소 이격거리를 1.5 m 이상으로 유지, 설치됨.

2.2.5 무정전 전원 공급

어떠한 경우에도 전원 공급이 중단되지 않도록 안전 계통의 주요 기능에 관련되는 설비에는 무정전 전원 및 비상 발전기로부터 전원이 공급됨.

2.2.6 채널의 전원 분리 및 다중화

채널별 전원은 크게 even, odd line으로 부터 공급함은 물론 3개 모선으로 나누어 공급됨.

2.2.7 Fail Safe

전원 및 제어용 공기 상실시 원자로를 안전한 정지 상태로 유도되도록 설계됨.

2.2.8 채널의 예비 전원 확보 및 자동 전환

주 전원 공급 장치의 기능 상실시 자동으로 예비 전원이 투입됨.

2.2.9 보호 계통 그룹별 기기 위치의 층별 분리

그룹1 과 그룹2 와의 안전 계통 설비 위치를 층별로 분리 설치됨.

2.2.10 내진.내환경 설계

보호계통 설비는 지진 및 환경(방사선, 열, 습도등)에 의한 영향을 고려하여 설계됨.

3. 원자로 보호 계통 주요 설계 변경

3.1 내 용

3.1.1 SDS(Shut Down System) 1 & SDS2 low level steam generator trip instrument

redundancy(DC #1)

월성 1호기는 각 원자로 정지계통에서 증기발생기 수위(총 4군데)를 각각 2 곳에서 측정하였으나 각 증기발생기 4대 모두에서 SDS1, SDS2 증기발생기 저수위 트립변수를 설정하여 감지.

3.1.2 SDS 2 On-line Poison Concentration Monitoring(DC #2)

월성1호기는 주기적(수동)으로 시료를 채취하여 소내 화학실험실에서 개돌리늄 농도를 측정하였지만 월성 2,3,4에서는 발전소 제어용 전산기(DCC)를 이용하여 연속적으로 Poison Tank내 전도도(conductivity)를 측정하여 질산 Gd. 농도를 온라인으로 모니터링하여 액체 독물질 주입 계통(LISS)의 신뢰도를 높임.

3.1.3 SDS 2 Trip for partial loss of flow(DC #3)

한 대의 열 수송 펌프(PHT P/P) 트립으로 인한 "partial loss of flow"를 검출하기 위하여 월성 1호기에서는 열수송계통의 출구 모관(outlet header) ROH #1, #5 두 군데에서 열 수송계통 고압력(PHT High Pr.)을 모니터링 했으나 출구 모관 4군데(ROH 1,3,5,7) 모두에서 "PHT High Pressure" 을 감지하여 결국 4군데 모두에서 High & Low 압력 신호를 감지하는 것이다. 그리고 추가적으로 일정 시간을 가지고 동작하는 지연 정지 기능과 원자로 출력 70 %이하에서 원자로 정지가 발생하지 않도록 하는 기능을 가짐.

3.1.4 SDS 2 Equipment Room(R-113) rearrangement(DC #4)

기존 원자로 제 2 정지 계통 관련 전송기가 설치되어 있는 기기실(R-113)이 복잡하고 설계개선, 변경으로 인한 전송기가 추가되어 기존 두개의 전송기가 설치되어 있는 랙(rack)을 신설된 기기실인 S-031, -031A에 기존 계측 설비와 함께 재 정렬하여 설치.

3.1.5 Shutdown System Software QA requirements(DC #5)

원자로 정지 계통 컴퓨터(PDC)에 대한 캐나다 원자력 규제 기관(AECB)의 소프트웨어 품질보증 요건 강화 및 새로운 하드웨어 선정에 따른 안전 계통 소프트웨어의 확인 및 검증작업.

3.1.6 High moderator temperature trip on SDS 1(DC #6)

기존 월성 1호기는 감속재 관련 변수로서 원자로 출력 연속 감발(Set-back)의 감속재 고온도, 출력 단계 감발(Step-back)의 감속재 고수위 변수를 설정하여 운용 중인데 이에 추가적으로 원자로 제 1정지 계통에 감속재 고온도 트립 변수를 설정하여 "loss of service water flow"를 대비.

3.1.7 Low power auto-conditioning for several trips on SDS1 and SDS2(DC #7)

기존 월성 1호기에서 발생할 가능성이 있는 원자로 저 출력시의 트립 해제 기능을 운전원이 수동으로 핸드 스위치에 의해서 이루어 졌는데 2호기에서는 PDC 프로그램에 의해서 자동으로 원자로 저 출력시 관련 트립 변수의 트립 기능 해제.

3.1.8 Programmable Digital Comparator(DC #55)

월성 1호기 원자로 정지 계통 전산기, PDC(Programmable Digital Comparator) 의 제작자인 미국 Data General 사의 제작 중단으로 새로운 하드웨어로 변경하여 SDS 1의 ABB 사의 P10, SDS 2는 PEP Modular Inc.의 VM 30으로 선정(공급자는 Marsh Instrumentation Inc. 임).

3.1.9 Display Local Error Message of PDC in MCR(DC #79)

현장(SCA, CER)에서 생성된 경보 내용을 주제어 실에서 운전원이 볼 수 있게 한 것으로서, DCC Contact Scanner를 이용하여 25 " CRT 에 경보 내용이 생성되게하여 현장에 가서 확인하지 아니하여도 용이하게 고장 및 이상 정보를 파악.

3.1.10 ECC Control Panel Modification(DC #11)

주제어실 PL-3에 위치한 비상 노심 냉각 계통(ECCS)관련 판넬의 공간 협소로 AECB 설

계 요건인 Man/Machine Interface 사항을 만족하기 위하여 1개 판넬에 설치되어 있는 관련 계측 지시기를 인간 공학적 측면을 고려한 2개 판넬에 분산, 조정하여 재배치.

3.1.11 Additional ECC Heat Exchanger(DC #12)

ECC 계통의 이용률 향상을 위하여 100% plate형 열교환기 1대 및 온도감시 회로를 추가

3.1.12 ECC Leakage Collection Improvement(DC #13)

냉각재 상실 사고(LOCA)시 비상 노심 냉각 계통 운전 중에 계통이 누설하여 Service 건물 접근 가능 및 종사자의 방사선 피폭의 위험도를 줄이기 위한 누설 회수 설비가 신설.

3.1.13 Improvements to ECCS Unavailability(DC #15)

ECC 계통의 전체적인 availability 향상을 위하여 계통 주입 파이프의 체크 밸브를 시험 가능한 공기 구동 체크 밸브로 교체하고 ECC Water 탱크 저 수위시 고압주입 밸브 "CLOSE" 신호 논리 회로의 이중화 및 후단시험 밸브의 동시 "CLOSE"를 위한 논리 신호제공, 증기 발생기 crash cool down 기능을 보증하기 위한 주증기 안전 밸브의 최소 개방 수량을 16개중 10개에서 7개로 감소, 다우징 탱크 흡입밸브와 관련한 ECC 펌프 연동 신호 제거 및 적절한 재 순환 유량 확보 등을 통해 계통의 신뢰도 증진.

3.1.14 Improve HTS Liquid Relief Valves Control Circuit(DC #69)

SDS 1의 기존 "PHT Flow Low" test loop의 안전 계통 정기 시험(SST)시에 사용하는 핸드 스위치인 HS-1D 혹은 HS-1F의 접점 접촉 불량으로 비정상적인 열수송 계통의 액체 방출 밸브(LRV)의 개방을 유도하고 있으므로 관련 제어 회로로부터 LRV 모니터닝 회로 및 휴즈 위치를 분리, 독립하고 필요시 경보를 알리는 LED를 SDS #1 판넬에 설치하여 관련 루프를 개선.

3.1.15 Shutdown System Loop Additional Isolation Valve(DC #81)

SDS 1의 기존 "PHT Flow Low" test loop의 안전 계통 정기 시험(SST)시 관련 루프의 공기 구동용 시험 밸브에서 침전물의 축적으로 인해 누설이 발생하여 공기 구동용 밸브 입력단에 필터를 설치, 침전물 축적 방지.

4. 기능 프로그램 사양서(Functional Program Specification)

중수로의 원자로 보호 계통은 12대의 Microcomputer에 의해 구성되고 이들 컴퓨터 는 6대씩 1개 그룹이 되어 SDS1과 SDS2를 구성하고 이들 각 채널(SDS1은 D, E, F/ SDS2는 G, H, J)은 2대의 독립된 PDC(Programmable Digital Comparator)로 구성된다.

과거의 아날로그 계산 장치로는 트립 조건 설정 및 원자로 출력에 따른 트립 설정치 변화를 유연하게 수행하기에 부족함이 있었다. 이에 따라 월성 2호기에서 운영할 컴퓨터는 고유의 아날로그 방식으로 수행하기 어려운 트립 로직에 사용하여 그의 기능을 수행한다.

각 컴퓨터의 기능은 Process Trip Parameter 관련된 Process신호들을 감지하여 원자로 운전 조건 즉 원자로 출력이나 열수송 계통펌프(PHT Pump)의 운전모드(즉4pump혹은2 pump) 에 따른 트립 설정치(Trip Setpoint)를 PROM(Programmable Read Only Memory)속에 실장된 프로그램에 의해 자동으로 계산하고 감지된 Process신호들과 자동으로 계산된 트립 설정치와 비교하여 이를 벗어나는 경우, 해당 원자로 정지 메커니즘(정지봉/질산개돌니늄)을 구동하기위한 동작 신호를 트립 로직에 보내 원자로를 긴급히 정지시키는 것이다.

이처럼 중수로 원자로 보호 계통에 있어서의 컴퓨터(PDC)의 역할은 중요하며 기본이 된다고 하겠으며, 원자로 보호 계통의 계측 제어 분야에 컴퓨터를 적용하여 원자로 기본 보호 계통(SDS#1,#2)을 구현한 전산 시스템에서 수행하고 있는 프로그램은 원자로 보호 계통에서 아주 중요한 역할을 하고 있는 것이다. 이에 따라 하드웨어적인 고찰 보다 소프트웨어적인 것에 중점을 두어 기능 프로그램(Functional Program)의 사양에 대해 기술하고자 한다.

4.1 내용

컴퓨터(PDC)에 의해서 수행되는 기능 프로그램(Functional Program)은 아래와 같은 내용으로 계통 설계자(System Engineer)에 의해 작성되어 이를 기본으로 하여 소프트웨어를 구현한다.

. General Concepts
- PDC 입출력(Input/Output)
- 트립 변수: 불 합리(Irrational), 즉시(Immediate), 지연(Delayed) 트립
- 원자로 출력 및 펌프 모드에 의존한 트립 설정치
- 저 출력시 트립 조건 해제
- 불합리한 신호 및 High Spread 경보
- PDC 감지 장치(Watchdog Timer)

. Self-Checks and Error Annunciation

- 프로그램 체크썸(Checksum)
- 소프트웨어 순차 점검(Sequence Check)
- Analog 계통 루프 점검(Wraparound Check)
- Digital 계통 루프 점검(Wraparound Check)
- 채널 동일성 점검(Identity Check)
- PDC 감지 및 에러 메시지(Error Message) 장치 시험

. PDC1 & PDC2 Common Functionality
- 펌프 모드 선택
- 이온 검출기(Ion Chamber) 출력 대수(Log) 값
- 중성자속 검출기(Flux Detector) 보상 평균 출력
- 이온 검출기 보상 선형(Linear) 출력
- 보상 출력값(Compensated Power Values) 비교

. PDC1 Trip Parameters
- 열 수송 계통 저 유량(SDS1), 열 수송 계통 저 차압(SDS2)
- 가압기 저수위(SDS1/SDS2)
- 증기 발생기 저수위(SDS1/SDS2)
- 감속재 고온도(SDS1)

. PDC2 Trip Parameters
- 열 수송 계통 고 압력(SDS1/SDS2)
- 열 수송 계통 저 압력(SDS1/SDS2)
- 증기 발생기 급수관 저 압력(SDS1/SDS2)

4.2 PDC 설계 특징

월성 2호기 PDC 의 주요 설계 특성은 다음과 같다.

ㅇ 기기의 구성 및 기능 면에서는 월성 1호기와 유사하나 입력 신호의 수가 증가되었고 일부변수의 트립 설정치 변경 및 트립 변수(SDS1의 감속재 고온도 변수) 설정.

ㅇ "PHT High Pressure"(SDS1/SDS2) 및 "PHT △P Low"(SDS2) 트립 변수에 delayed trip 기능이 추가됨.

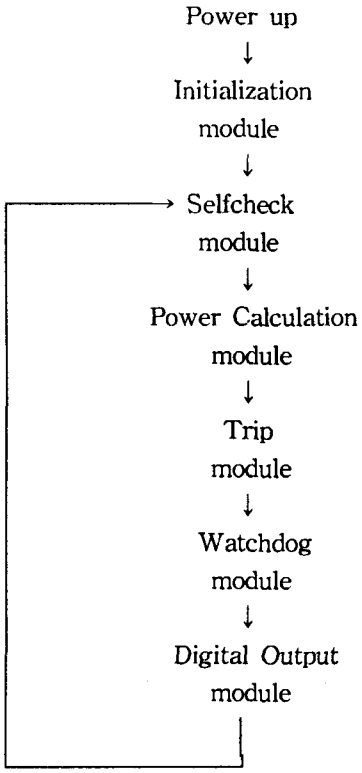
ㅇ 일부 트립 변수에서 원자로 출력이 저출력일때 트립 조건이 되더라도 트립이 되지 않게 하는 기능을 보완하였는데 이는 월성 1호기에서는 이온 검출기의 대수(Log) 출력 값만 고려하

였는 데 반하여 2호기의 입부 변수는 이온 검출기의 대수 출력 값에 중성자속 검출기 평균값을 함께 고려하여 적용함.

ㅇ 새로운 컴퓨터 하드웨어 기종 사용

ㅇ 캐나다 원자력규제기관(AECB)의 소프트웨어 품질보증요건 강화 및 새로운 하드웨어 선정에 따른 안전계통 소프트웨어의 확인 및 검증

4.3 프로그램 구성(Program Organization)



4.4 소프트웨어 설계에서 고려해야 할 사항(Software Design Considerations)

소프트웨어 설계는 AECL의 Safety Software design group에서 작성한 "PDC Quality Project Plan" 의 절차에 따르는데 원자로 제2 정지 계통(SDS2)의 설계시 고려해야 할 사항에 대해서 기술한다.

4.4.1 두개의 PDC 사용

하나의 채널에 두 대(PDC 1 & 2)의 전산기를 사용하여 각각 서로 다른 독립적인 기능을 수행하며 프로그램이 저장되어 있는 PROM 장치에는 기능상 차이가 있는 채널간에 상호 교환하여 사용이 되지 않도록 방지장치(채널 Identity check 등)가 되어 있다.

4.4.2 트립 타이밍(Trip Timing)

트립 변수용 디지털출력(D/O)은 트립 동작점에 도달되면 ADC(Analog Digital Converter)에 신호가 수신되면 100 msec 이내에 개방되어야 한다. 지연 트립(delayed trip)에 대한 시간요건은 각 트립 변수에 따라 정해진다.

4.4.3 트립 변수의 독립성(Independence of trip parameters)

트립 변수들은 입력 신호 혹은 출력 신호의 공유 경우를 제어하고는 기능상 독립성을 가진다. 특히 공정 계통 트립 이후 다른 트립 기능은 유효하게 계속적으로 그 기능을 수행하여야 하며 모든 경보 및 지시 장치의 기능도 상실해서는 안된다.

4.4.4 불합리한 아날로그 신호(Irrational Analog signal) 취급

일반적으로 불합리한 경보(alarm) 설정치는 아날로그 입력 신호의 정상 동작(교정) 범위를 약간 벗어난 범위에서 설정되어 있다. 그래서 정상 동작 범위를 현저하게 초과하는 경우에 경보가 발하도록 되어 있고 과도 혹은 정지 상태에 따른 불필요한 경보 발생을 줄 일수 있다. 50 mV 히스테리시스(Hysterics) 떨림(dithering)을 방지하기 위해 비정상 경보 한계치(irrational alarm limits)와 퍼짐 검사 경보(spread check alarm) 한계치에 적용되어 보다 안전한 방향으로 동작하게끔 한다.

예를 들면, 낮은(low) 불합리한 경보 동작점이 850 mV 인 경우, 경보는 850 mV 값에 도달하거나 그 이하일 때 발생하게 된다. 그러나 경보 해제는 그 신호가 900 mV 이상 올라 갈 때까지 해제되어서는 안된다. 같은 방법으로, 높은(high) 불합리한 경보 동작점이 4550 mV이라고 할 때 경보는 4550 mV에 도달하면 발생하나 경보의 해제는 4500 mV이하까지 떨어지지 않으면 해제되지 않는다. 그리고 단일 트립 변수 중에서 한 개 이상의 아날로그 입력값이 PDC 로 들어올 경우 그 신호에 대해 퍼짐 검사(spread check)가 시행되는데 이는 그 신호 그룹에서 현재 가장 높은 신호 값과 현재 가장 낮은 신호 값과의 절대 비교 차이 값으로 정의되고 필요시 경보를 발한다.

4.4.5 에러 계산 및 오차(Calculation Error & Tolerance)

원자로 출력에 의해 결정되는 트립 설정치는 ± 1% FP내의 정확도를 가져야 한다.

4.4.6 초기화(Initialization)

PDC가 초기화되면 각 트립 변수들은 어떠한 입력도 받지 못하므로 트립이 되어 안전한 방향으로 가며 트립, 경보창 및 에러 메시지용 D/O는 개방되고 표시용 아날로그 출력은 0 volt로 되어 지시 값은 영점 이하로 떨어져야 한다.

4.4.7 신뢰도 요건(Reliability Requirements)

SDS2에 허용된 종합 비이용율(total unavailability)은 10^{-3}년/년이며, 부품(Component)단위 허용 비이용율은 10^{-4}년/년이다. 신뢰도는 고장-안전 정지 설계(fail-safe design),

그리고 자체 검사(Self-check) 및 진단(Diagnostic) 특성에 의해서 개선되었다.

4.4.8 Inclusive versus Exclusive Comparisons)

따로 명기되지 않은 한, 비교는 안전한 방향으로 이루어 져야 한다. 예를 들면, 트립 혹은 경보 조건으로 아날로그 입력을 상한 제한치와 비교할 경우는 input ≥ high limit 을 반면에 하한 제한치와 비교할 경우에는 input ≤ low limits 을 사용해야 한다.

4.4.9 분리 트립 설정치 제공(Provision of separate setpoints)

하나 이상의 계측 루프와 공유되는 상수 트립 설정치는 설정치 변화에 용이하게 대응하기 위해 메모리에 따로 분리 저장되어야 한다.

5. 결론

이상과 같이 본 논문에서는 기존 운전 중인 발전소 중에서 디지털화가 가장 많이 된 중수로형 발전소의 원자로 보호 계통을 개선한 월성 2호기 신기술을 고찰해 보았다. 우리 나라에서도 원전 계측 제어 분야의 설계 개선의 필요성이 요구되는 시점에서 특히, 발전소 보호(안전)계통에 본 논문에서 기술한 입증 설계개량 기술을 적극적으로 활용하여 원자로 보호 계통을 보다 진보된 개량 디지털 보호 시스템을 구축하였다. 특히 향후 중수로 후속기 도입에 대비하여 적용성 및 설계개선 기술을 사전에 검토하여 관련 기술을 축적해야 한다. 이를 위하여 컴퓨터의 원자로 보호 계통 적용에 대한 계통설계, 그에 따른 하드웨어 개발 및

국내 인 .허가 기준에 따른 소프트웨어 확인 및 검증 기법 개발은 관련 제반 기술에 대한 연구와 개발의 병행 작업이 요청되고 특히 원자로 보호계통에 있어서의 컴퓨터 기능 프로그램의 역할은 매우 중요하므로 설계시 필요한 요구 및 기능 요건을 설정하고 확립하는 등 관련 기술을 축적해야 한다.

참 고 문 헌

1. Conceptual Design Description, CANDU Safety Presentation, Dec. 6 - 7, 1991
2. 86-68200-PFS-000, SDS1 PDC Program Functional Specification
3. 86-68300-PFS-000, SDS2 PDC Program Functional Specification
4. 59-68300-257-200 Rev. 2, PDC Program Functional Specification,
5. FSAR, Vol. 5, Wolsong NPP Unit No. 2/3/4
6. 86-68300-DM-003, SDS2 Trip Logic and Test Circuitry
7. 59-68200-258-100, PDC Program Description for SDS1
8. N. M. Ichiyen, P. K. Joannou, safety Critical Software design approaches used by AECL and OH