

발전소감시경보계통 개발 Development of the Plant Monitoring and Annunciator System

정기훈, 이정권, 조주현, 백승민, 김항배
한국전력기술(주)
대전광역시 유성구 덕진동 150

이순형, 인식련
한국수력원자력(주)
서울시 강남구 삼성동 167

서호준, 이순성
BNF 테크놀로지(주)
대전광역시 유성구 덕진동 150

요 약

발전소감시경보계통은 한국형 표준원전의 발전소감시계통과 발전소경보계통을 통합한 종합적인 감시 및 경보계통이다. 발전소감시경보계통은 한국형 표준원전과 비교하여 새로운 설계 특성을 적용하고 있으므로 프로토타입 개발을 통하여 변경된 설계 사항에 대하여 성능 및 설계 타당성 검증이 필요하다. 본 논문에서는 한국표준형원전 설계개선 2 단계에서 개발된 발전소감시경보계통의 설계 내용과 기능을 설명하고, 관련 기능 요건과 성능을 검증하기 위해 개발된 프로토타입에 대하여 기술하였다.

Abstract

The Plant Monitoring and Annunciator System (PMAS) is an integrated monitoring and annunciation system that combines the existing Plant Monitoring System (PMS) and Plant Annunciator System (PAS) for the Korea Standard Nuclear Power Plant (KSNP). The PMAS design needs verification of performance and design validity through prototype development because the design concept of PMAS differs from that of the PMS/PAS in the KSNP in many respects. This paper addresses the design concept and functional characteristics of the PMAS and describes the prototype activities which are developed to verify the functional requirements and performance of the PMAS.

1. 서론

한국형 표준원전의 발전소감시계통(PMS)은 발전소의 운전상태를 실시간으로 감시하는 계통으로 미국 Westinghouse Electric Company사와 한국전력기술(주)이 공동으로 시스템을 개발해오고

있으며, 발전소경보계통(PAS)은 발전소의 이상상태를 운전원에게 신속하게 알려주는 계통으로 영광 원전 5,6 호기부터 국내 기기제작업체에 의해 제작 납품되고 있다. 한국형 표준원전은 PMS 와 PAS 의 분리 설계에 따른 경보의 불일치 문제, 필수안전기능감시계통(CFMS)과 비상운전절차서(EOP) 사이의 일부 불일치 문제, 발전소 표준시각에 의한 시각 동기화의 미적용 문제 등이 있었고, 이러한 문제점을 보완하고 기능 및 경제성을 개선하기 위하여 발전소감시경보계통 (PMAS, Plant Monitoring and Annunciator System)을 개발하게 되었다. 본 논문에서는 통합설계에 따른 규제요건 및 설계대응, 경보 설계, SOE 신호처리 설계, 통신망설계 등과 관련된 기본설계 요건을 설명하고, 국내외 타원전의 유사 시스템과 비교분석을 통하여 PMAS 에 대한 설계 세부사항을 기술하였다. 또한 통합에 따른 설계의 시현성 검증을 위하여 개발한 프로토타입의 설계와 구현에 대한 세부사항도 본론에 기술하였다.

2. 본 론

2.1 규제요건 및 설계 대응

PMAS 는 NUREG-0800, Section 7.5 에서 안전에 중요한 정보계통으로 정의되어 있는 경보계통과 BISI (Bypassed or Inoperable Status Indication), 그리고 Section 7.5 및 경수로형원전 안전심사지침 제 18.2 절에서 정의되어 있는 SPDS (Safety Parameter Display System), ERF (Emergency Response Facilities), NDL (Nuclear Data Link)을 포함하는 계통으로서, 각 계통들에 대하여 별도로 부과되어 있는 규제 요건들을 모두 만족해야 하는 시스템이다^{1),2)}. 표준원전의 경우는 경보계통과 BISI 는 발전소경보계통에, 안전변수지시계통은 발전소컴퓨터계통에 포함되어 별도의 계통으로 분리 설계됨으로써 인허가 관점에서 해당 계통에 따라 개별적으로 대응해왔으나, PMAS 의 경우는 두 계통이 통합됨에 따라 상기의 모든 인허가 요건에 부합하기 위한 종합적인 검토가 필요하다. 따라서 현재의 규제요건 상의 주요 요구사항 및 이를 만족하기 위해 인허가 관점에서 고려된 설계 내용은 다음과 같다.

2.1.1 경보계통 요건

최근 디지털 컴퓨터의 사용으로 인해 인허가 관점에서 경보계통의 중요성이 대두되고 있고, 발전소 현장에서의 경험을 바탕으로 경보계통에 EPRI URD 요건을 적용하여야 한다는 입장이 대두되고 있으며^{4),8)}, SECY-93-087 의 I.T 항에서 ALWR 경보계통에 대한 추가요건으로서 EPRI URD 요건을 적용한다는 입장을 명시하였다³⁾. 이후 국내 신규원전의 안전성 평가 기준으로 사용되는 NUREG-0800, Section 7.5 에서도 다중성(Redundancy), 다양성(Diversity), 시험성(Testability), 품질수준(Quality Levels) 측면에서 경보계통이 비록 안전계통은 아니지만 운전시 중요한 정보계통임을 감안하여 정상 및 비정상운전을 지원하기에 적절한 신뢰성을 갖는지를 평가한다¹⁾는 입장을 제시하고 있으며 이에 대한 대응 방안은 다음과 같다.

- 보호계통과 연계되는 입력부분은 격리장치 요건 만족
- 품질보증 프로그램을 작성하고, 안전에 대한 중요도를 고려한 적절한 품질 기준에 따른 설계, 제작, 건설, 시험, 검사
- 경보계통 소프트웨어의 확인 및 검증⁵⁾ 수행
- 운전 중 경보계통의 자체시험 기능 제공
- 센서를 제외한 I/O 카드, 통신기기, 컴퓨터 등 모든 기기를 이중화 구조로 구성
- 경보창 경보기능 전체의 작동불능에 대비하여 경보창과 독립적인 경보처리 기능 및 경로

(Path)를 갖는 경보 Backup 기능을 추가하여 경보계통의 신뢰성 강화

- 동일 경보에 대해 경보창과 CRT 로 다양한 표시수단을 제공하여(Diversity) 컴퓨터 기반 경보 표시기능의 공통원인 고장에 대비

2.1.2 BISI 요건

NUREG-0800, Section 7.5 에서 BISI 에 포함되어야 하는 최소한의 정보로서 RTS 및 ESFAS, RCS 의 저압격리용 연동장치, ECCS Accumulator 격리밸브, 안전주입 재순환 제어 등에 대한 정보 지시를 요구하고 있으며¹⁾, RG 1.47 에서 권고하고 있는 바와 같이 주제어실에서 BISI 의 자동지시 기능 및 계통 수준 BISI 지시기의 수동작동 수단을 제공해야 한다⁵⁾는 입장을 제시하고 있다. 이에 대한 대응 방안으로서는 상기 요건들을 기존의 표준원전에서 이미 만족하고 있으므로 PMAS 에서도 이를 준용하여 동일한 설계개념을 적용한다.

2.1.3 SPDS 요건

SPDS 는 NUREG-0800, Section 7.5 에서 요구하는 격리요건에 따라 보호계통으로부터 격리 되도록 설계⁴⁾되어야 하며, 경수로형원전 안전심사지침 제 18.2 절에서 주제어실 내의 운전원이 이용하기 편리한 위치에 설치되어 노심반응도 제어, 원자로심 및 1 차계통의 열제거, 원자로냉각재계통 건전성, 방사능제어, 격납건물 건전성 등의 필수안전 기능에 대한 정보를 인간공학 원리에 따라 간결한 형태로 연속적으로 표시할 것¹⁾과, TMI 후속조치 사항인 NUREG-0696 에서 고이용률을 만족할 것을 요구하고 있다⁷⁾. 특히 상기의 규제요건에서는 컴퓨터기반 계통의 신뢰성 확보를 위하여 적절한 시스템 확인 및 검증을 수행할 것을 요구하고 있다^{1), 7)}. 상기 요건들은 한국형 표준원전의 CFMS (Critical Function Monitoring System) 설계에서 이미 만족시키고 있으며, PMAS 에서도 이를 준용하여 동일하게 설계한다.

또한 올진 3,4 호기 인허가 과정에서 CFMS 와 비상운전절차서 사이의 일부 불일치 사항에 대한 인허가 기관의 지적 및 문제해결 요구가 있었다. 따라서 이들 요구 사항을 만족하기 위하여 기존의 CFMS 의 기능을 향상시킨 새로운 계통인 안전변수지시평가계통(Safety Parameter Display and Evaluation System; SPADES)을 제안하였다⁹⁾. SPADES 는 비상운전절차서를 수용하고 인간공학적 요소들을 더욱 강화하여 설계하였다.

2.1.4 ERF, NDL 요건

ERF 및 NDL 은 발전소의 비정상 상태에서 외부 기술 지원팀이 발전소 안전에 관련된 중요 변수들에 대한 정보를 이용하여 안전상태를 분석할 수 있도록 관련 데이터를 전송하는 기능으로서, NUREG-0800, Section 7.5 의 격리요건에 따라 보호계통으로부터 격리되도록 설계할 것을 요구하고 있으며⁴⁾, 이 요건은 기존 표준원전에서 데이터 전송경로가 광통신 네트워크를 통해 격리됨으로써 기 만족되고 있으며 PMAS 에서도 동일한 설계개념을 적용한다.

따라서, PMAS 는 현재 발전소감시경보계통에 적용되는 모든 규제 요건을 만족하도록 설계된다.

2.2 기본설계

2.2.1 경보설계

PMAS 의 경보설비는 한국 표준형 발전소에서 경보계통과 발전소 컴퓨터 계통간의 분리설계에 따른 두 계통간의 경보 및 인간공학적 표시의 불일치를 해소하여 일관된 경보정보를

제공하고, 경보 기능 및 운전원 지원기능을 강화하여 이용률을 향상시키도록 설계하고 있고, 같은 현장의 경보접점을 감시하지만 경보계통 고장으로 인한 운전정보의 손실을 최소화 하기 위해 기능적으로 독립된 다중시스템으로 설계한다. 또한, 경보창 및 CRT를 통한 정보 표시를 다양화 함으로써 다중성, 다양성에 근거한 설계를 적용하여 신뢰성 있는 경보정보를 제공하도록 설계한다.

또한, PMAS 경보계통은 발전소의 안전 및 비안전 관련 경보신호와 SOE 입력 신호의 주기적인 감지, 비안전 관련 경보신호의 단자대 제공, 안전 관련 입력과의 격리 제공 및 비안전 현장 경보신호의 원격 멀티플렉싱 기능을 제공하고 자동 실시간 진단 기능으로 계통 내부의 고장을 감지할수 있도록 진단 정보를 운전원에게 제공하여 고장으로 인한 운전 불능 상태를 최소화 하도록 설계한다.

PMAS 경보계통은 발전소 조건에 부합되는 경보 논리 및 설정치, 중요도 및 신속성에 따른 우선 순위 부여 등의 경보처리 알고리즘을 적용하여 운전원에게 우선 순위에 따른 경보를 제공함으로써 운전원의 운전부담을 줄일 수 있다. 또한, 안전에 중요한 변수 및 그 변수에 대한 설정치를 총괄적으로 관리하고, 이를 이용하여 하부계통으로부터 입력되는 각종 정보를 처리하고 있으므로 필요시 변경이 가능하고, 다중의 통신망 구조로 설계되어 고장난 기기는 온라인 상태에서 손쉽게 교체할 수 있으므로 고유기능의 상실이나 손실 없이 기기의 유지/보수가 용이하여 발전소의 가용성을 증대 시킬 수 있다.

2.2.2 SOE 신호설계

Sequence of Event (SOE) 계통은 발전소 운전 정지 발생시 신속히 그 원인을 추적 규명하여 발전소 정지 시간을 최대한 단축할 수 있도록, 운전정지 원인 파악에 유용한 디지털 신호를 SOE 입력으로 구분하여 처리 한다. 이 계통은 사고 또는 비상정지 상태가 발생한 이후에 그 장소와 시간 등에 대한 정보를 순차적으로 기록하는 기능을 갖는다. 그 성능은 분해능이 1ms 로 사고시 원인규명을 위한 유용한 설비로 이용될 수 있도록 설계한다.

SOE 계통은 발전소경보계통(PAS)에 포함되며, Input Scanner Cabinet(INSC)-A1 및 B1 캐비닛에 신호 입력카드, 전용 SOE 프로세서와 통신모듈로 구성된다. 비안전계통에서 발생하는 사고 신호들은 실배선 케이블이 Termination 캐비닛에서 2 개의 신호로 분기되어 이중화된 INSC-A1 및 INSC-B1 캐비닛에 연결되고, 안전계통에서 발생하는 SOE 신호는 PAS의 Isolation 캐비닛을 거쳐 신호가 분기된후 이중화된 INSC-A1 및 B1 캐비닛에 각각 입력된다. SOE 입력신호는 NSSS 및 BOP 신호에 대해 충분한 여유분을 포함하여 총 800 개까지 처리할 수 있도록 설계되어 있으며 이중 160 여개 신호는 경보신호로도 사용된다. 각각의 INSC 캐비닛에서 처리된 SOE 데이터는 Input LAN 을 통해 PCS (Plant Computer System)의 경보서버 및 시스템서버에 전달된다. SOE Processor 는 독립 모듈로 구성되고 전용 SOE 신호입력카드를 거쳐서 처리되므로 그 처리과정이 단순화되어 시간지연을 최소화하도록 설계하였다.

SOE 처리를 위한 두 캐비닛의 동기화는 Time LAN 에 의해 처리된다. SOE 프로세서는 동기된 시간을 기준으로 입력된 SOE 신호에 대해 Time-tagging 을 한다. PCS 서버에서 두개의 INSC 캐비닛에 있는 SOE 프로세서들로부터 Input LAN 을 통해 사고신호 정보를 수신하고, 분류(sorting) 알고리즘을 이용하여 SOE 발생시간 순서에 따라 재정렬하여 SOE 보고서를 생성한다. 작성된 SOE 보고서는 Event 프린터를 통해 출력되고 파일로도 저장된다. 출력 저장된 파일은 승인된 관리자 이외에는 삭제가 불가능하다.

2.2.3 통신망설계

PMAS의 하부 계통인 PDAS, PAS, PCS는 Input LAN과 System LAN 등 2계층의 LAN에 연결되어 통신한다. Input LAN은 주로 PAS의 SOE, 경보 입력 및 PDAS(Plant Data Acquisition System)에서 처리된 아날로그, 디지털 입력이 TCP/IP 또는 UDP/IP 프로토콜을 이용하여 PCS 서버와 경보창으로 전송되도록 이중화되어 있으며, System LAN은 PCS 서버, 디스플레이, 프린터등과 일부 NSSS 및 BOP 연계 계통으로부터 입력신호가 TCP/IP 통신을 통해 전송되도록 이중화되어 있다. System LAN은 디스플레이, 기록, 계산 및 응용 프로그램의 기능을 수행하기 위해 필요한 정보를 교환하기 위한 통신망이다. Input LAN과 System LAN의 정보교환은 게이트웨이를 통하여 통제됨으로써 각 통신망의 고유한 기능 수행시 최대의 안정성을 갖도록 하였다. 또한 상기 LAN 이외에, Time LAN은 발전소의 표준 시각장치를 기준으로 정밀한 시간 측정이 요구되는 하부 계통의 시각 동기화를 위하여 독립된 통신망으로 분리 하였다. Plant LAN은 PMAS 정보를 PMAS 외부로 제공하기 위한 통신망이다.

PMAS에서 시스템서버, 데이터서버 및 경보서버로의 입력을 제공하는 PDAS, INSC Cabinet, MUX. Cabinet, ICCMS 및 BOP 계통 등은 정상운전을 수행하기 전에 해당 서버로 접속하여 각 하부계통의 지역 데이터베이스를 다운로드 받아 초기화하도록 설계하였다. 각 하부계통은 다운로드 받은 데이터베이스를 근간으로 하여 PMAS 서버의 입출력 기능 및 내부 기능을 수행하도록 설계하므로 데이터베이스의 다운로드는 고신뢰성이 요구된다. 따라서 데이터베이스 초기화는 데이터 송수신의 신뢰성이 높은 TCP/IP로 수행 되도록 설계한다. 지역 데이터베이스 초기화가 완료된 후에는 현장 입출력 신호를 주기적으로 해당 서버 및 타 하부계통에 동일한 정보를 정해진 시간 내에 전달해야 하므로 응답시간을 최대한 향상시키고 효율적인 데이터 전달을 위해서는 1:N 통신을 사용해야 한다.

PMAS는 하부계통에서 취득한 현장신호를 UDP/IP 프로토콜의 브로드캐스팅 방식으로 Input LAN에 연결된 여러 계통에 동시에 전송하도록 설계한다.

2.3 타원전의 유사시스템 비교분석

PMAS 설계의 선행 조사로 발전소감시계통 및 경보계통에 대한 타원전의 유사 시스템을 조사하여 비교 분석하였다. 한국형 표준 원전인 울진 5,6 호기의 감시계통, 고리 1 호기 소내감시계통, Westinghouse사의 WDPF II에서 발전된 Ovation 시스템, Foxboro의 I/A(Intelligent Automation) 시스템, Siemens의 Teleperm XP, 그리고 CANDU 9 PDS(Plant Display System)를 비교 대상으로 선정하여 조사하였고 이를 PMAS 시스템과 비교하였다. 이러한 타원전의 유사 시스템과의 비교 분석을 통해 한층 진보한 개념의 시스템을 구축하는 방향으로 발전소감시계통 및 경보계통의 통합설계를 진행하였다.

2.4 시스템 설계

PMAS는 발전소자료수집계통, 발전소경보계통, 발전소컴퓨터계통으로 구성된다. PDAS는 발전소 여러 계통에서 수집되는 아날로그 및 디지털신호 등을 처리하여 PCS에 전송하며 또한 부적절노심냉각감시계통(Inadequate Core Cooling Monitoring System : ICCMS) 입력 신호와 고정노내검출기증폭계통(Fixed Incore Detector Amplifier System : FIDAS) 입력 신호를 처리하여 ICCMS 및 PCS에 전달한다. PAS는 현장의 경보 및 SOE 입력을 처리하여 PCS 및 경보창으로 신호를 제공한다. PCS는 NSSS의 일부 계통과 BOP의 일부 계통으로부터 입력되는 신호는 광통신 네트워크로 직접 전송받고 나머지 계통으로부터의 입력신호는 PDAS를 통하여 전송

받는다. 또한, PCS 는 입력신호를 처리하여 모니터, 지시계, 프린터 등을 이용하여 발전소 운전 정보를 운전요원에게 제공한다. KSNP+의 PMAS 계통 구성도는 그림 1 과 같다.

PMAS 는 가용도를 높이기 위해 서버들을 기능별로 분산형 구조로 구성하여 시스템 서버, 데이터 서버, 경보 서버들로 각각 이중화하고, 유지보수용 서버도 별도로 제공한다. 시스템 서버는 입출력 자료의 처리, 계산 및 응용 프로그램의 스케줄링 기능 등을 제공한다. 데이터 서버는 HDSR (Historical Data Storage and Retrieval)을 위한 저장기능을 제공하고 경보 서버로부터 전달된 경보 자료 등을 저장한다. 경보 서버는 경보처리와 함께 전용 경보 CRT 에 경보 메시지 등을 제공한다. 유지보수용 서버는 계통의 성능을 감시하고, 온라인 시험 및 진단, 경보논리 수정, 온라인 데이터베이스 수정 기능 등을 제공한다. 그래픽 디스플레이는 운전 지원기능, 운전상태 감시 기능, 기록 기능 등과 같이 MMI 관련한 모든 기능을 제공한다.

PMAS 경보계통의 경우 운전요원에게 독립된 기능 및 다양성을 제공하기 위해 이중화된 경보기능을 제공한다. 이들은 PAS 입력을 직접 받아 경보창에서 구현하는 PAS 경보 계통과 PCS 의 CRT 를 이용하여 구현하는 PCS 경보 기능으로 구분되고, 한쪽의 경보 기능이 상실 되더라도 나머지 경보 계통에는 영향을 주지 않으며, 정상운전시는 주기적으로 경보처리 결과를 상호 비교하여 경보에 대한 신뢰성을 높인다.

2.5 표준원전과의 주요 설계변경 사항

PMAS 는 1) PCS 와 PAS 사이에서 통합 이전에 있었던 경보표시의 일관성 문제 및 비효율성 문제를 해소하고, 2) 분산형 시스템구조로 구성하여 시스템 장애의 영향을 최소화하며, 3) 경보 표시의 다중화 및 실시간 운영체제의 사용으로 계통의 신뢰성을 향상시키며, 4) PCS 플랫폼을 서버급 워크스테이션에서 산업용컴퓨터로 다운사이징 (downsizing)하며 통합으로 인해 불필요한 중복 신호를 제거함으로써 경제성을 제고하고, 5) 향상된 운전원 지원 기능을 추가하여 유지보수성을 향상하고자 하는 측면에서 기능이 개선된 종합 정보계통으로서 표준원전에 대비한 주요 설계변경 비교사항은 표 1 와 같다.

2.6 프로토타입 개발

2.6.1 하드웨어

PMAS 는 기존의 PDAS, PAS 및 PCS 를 통합한 형태로 프로토타입 구성은 그림 2 와 같다. 이는 향후 건설될 신규호기의 사전 설계로 PMAS 소프트웨어 개발 및 시험, 장비 검증 등을 위해 기능적으로 구성된 설비이며 향후 계통설계, 소프트웨어 개발, 시운전, 현장요원 교육 및 핵연료 재장전시 소프트웨어 변경 등에 유용하게 사용가능 하다. PMAS 프로토타입은 PDAS, PAS, I/O 시뮬레이터, 게이트웨이, 유지보수용 서버, 경보서버 및 각종네트워크(Input, System, Time LAN)들로 구성되며 주요 부분은 이중화구조를 갖도록 설계하였다.

2.6.1.1 PDAS

PDAS 는 안전(채널 A, B, C, D) 및 비안전(채널 N1, N2) 채널로 구성되지만, 프로토타입에서는 채널 A 만 실제 발전소에서와 같이 Full Scope 으로 설계하여 A/D Conversion, Engineering Conversion 및 Signal Conditioning 을 하여 PCS 의 모든 서버에 관련 정보를 전달하고, 다른 채널들은 CPU Card 및 일부의 중요한 입력 Card(PI, FI 및 RTD)들로 신호를 모사하여 PDAS 고유의 기능을 수행하도록 설계하였다.

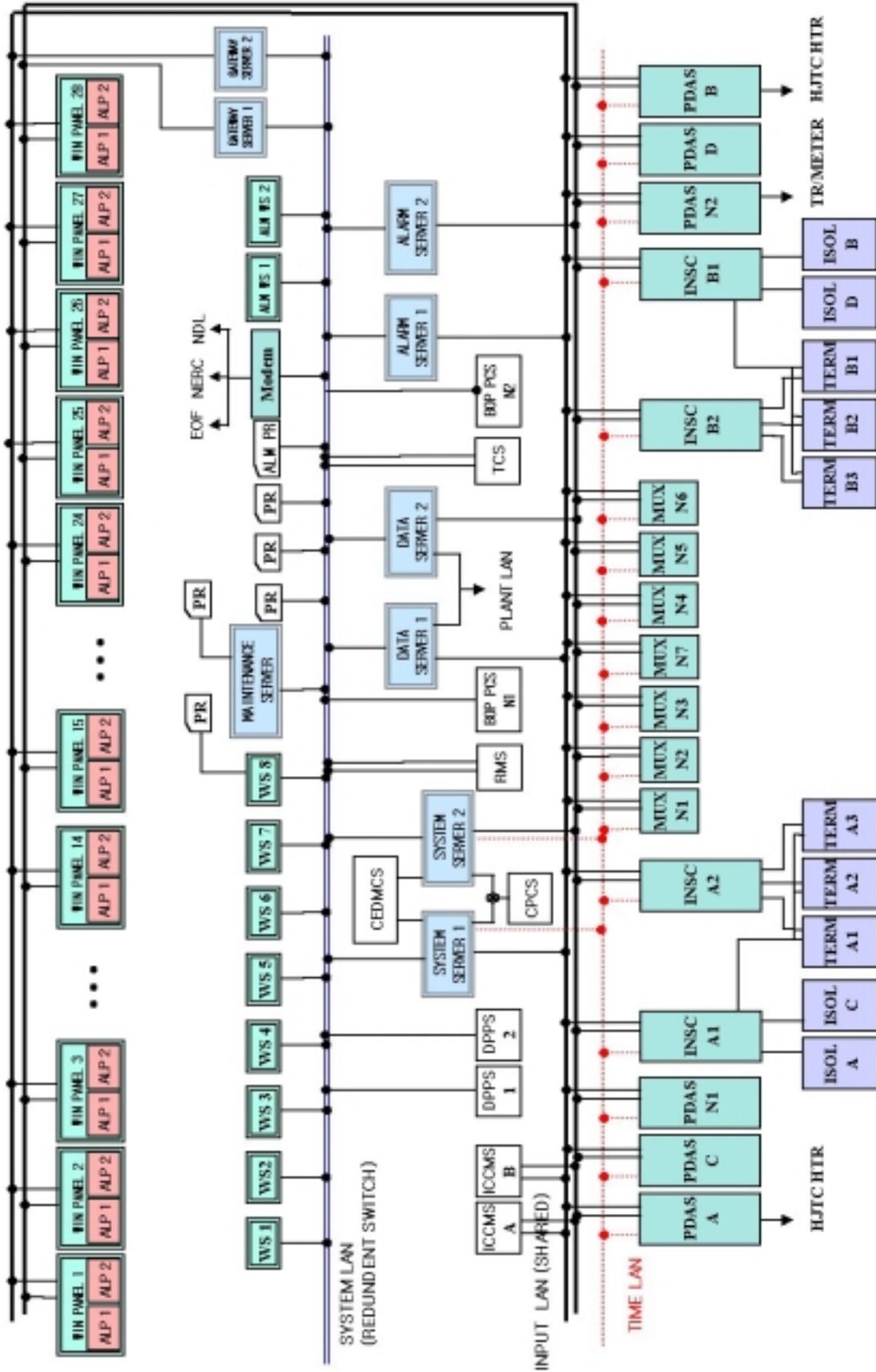


그림 1. PMAS 구성도

표 1. 표준원전과 PMAS 의 설계비교

비교 항목		표준원전	PMAS
시스템 및 하드웨어 설계	서버 시스템 구조	이중화된 단일 컴퓨터로 구성된 중앙집중 구조	이중화된 시스템서버, 데이터서버, 경보서버로 구성된 분산 구조
	서버 플랫폼	HP 워크스테이션	산업용컴퓨터
	네트워크 설계	단일계층 네트워크 구조로 TCP/IP, Serial DataLink 사용	2 계층 네트워크 구조로 TCP/IP, UDP/IP, Serial DataLink 사용
	SOE 설계	PDAS 에서 입력신호 처리, 처리 수량이 512 개로 제한	PAS 에서 입력신호 처리, 처리 수량을 800 개로 확장
	경보입출력 설계	PDAS 와 PAS 에 중복신호 존재	PDAS 로 SOE 신호입력을 제공하기 위해 사용하던 Aux. Relay Output Cabinet 제거 및 중복신호 삭제
	시각 동기화	직렬통신을 이용하여 자체 시각 동기화	표준시각설비 및 전용 Time LAN 을 이용한 시각 동기화
	Plant LAN 연계 기능	제공하지 않음	데이터서버를 경유하여 제공
	데이터저장장치	하나의 Tape 저장장치를 이중 서버가 공유	이중의 데이터서버 각각에 전용 Back-up Storage 를 설치
소프트웨어 설계	서버 운영체제	비실시간 운영체제	실시간 운영체제
	안전변수지시 기능	CFMS 와 비상운전절차서 사이의 일부 불일치 존재	CFMS 와 비상운전절차서 사이의 불일치 해결
	운전원 지원 기능	P&ID, 문서 View 기능 미제공	P&ID, 문서 View 기능 제공
		Hyper-Text Builder 기능 미제공	Hyper-Text Builder 기능 제공
		운전원 Shift Diary 기능 미제공	운전원 Shift Diary 기능 제공
		텍스트 형태의 제한된 시스템상태 표시	Mimic 형태의 시스템상태 표시
	경보 억제 기능	발전소 운전 모드에 따른 경보 억제 기능 미제공	발전소 운전 모드에 따른 경보 억제 기능 제공
	데이터베이스	표준원전의 데이터베이스 구조만 지원	플랜트 형태에 무관한 데이터베이스 구조를 지원하며, PAS 데이터베이스도 통합
	소프트웨어 유지 보수	Code 수준의 변경 필요	MMI 화면의 구성 변경만으로 수용
	소프트웨어 이식성	개발된 UNIX 운영체제 하에서만 동작하며 OS Version 에도 의존	대부분 POSIX 호환 함수만을 사용하므로, 하드웨어에 의존적인 일부 모듈에 대한 수정만으로 UNIX 계열의 모든 운영체제에서 동작 가능
경보창에 대한 Backup 표시	단순한 텍스트형태의 표시	경보창과 동일한 구성의 CRT 표시화면 제공	

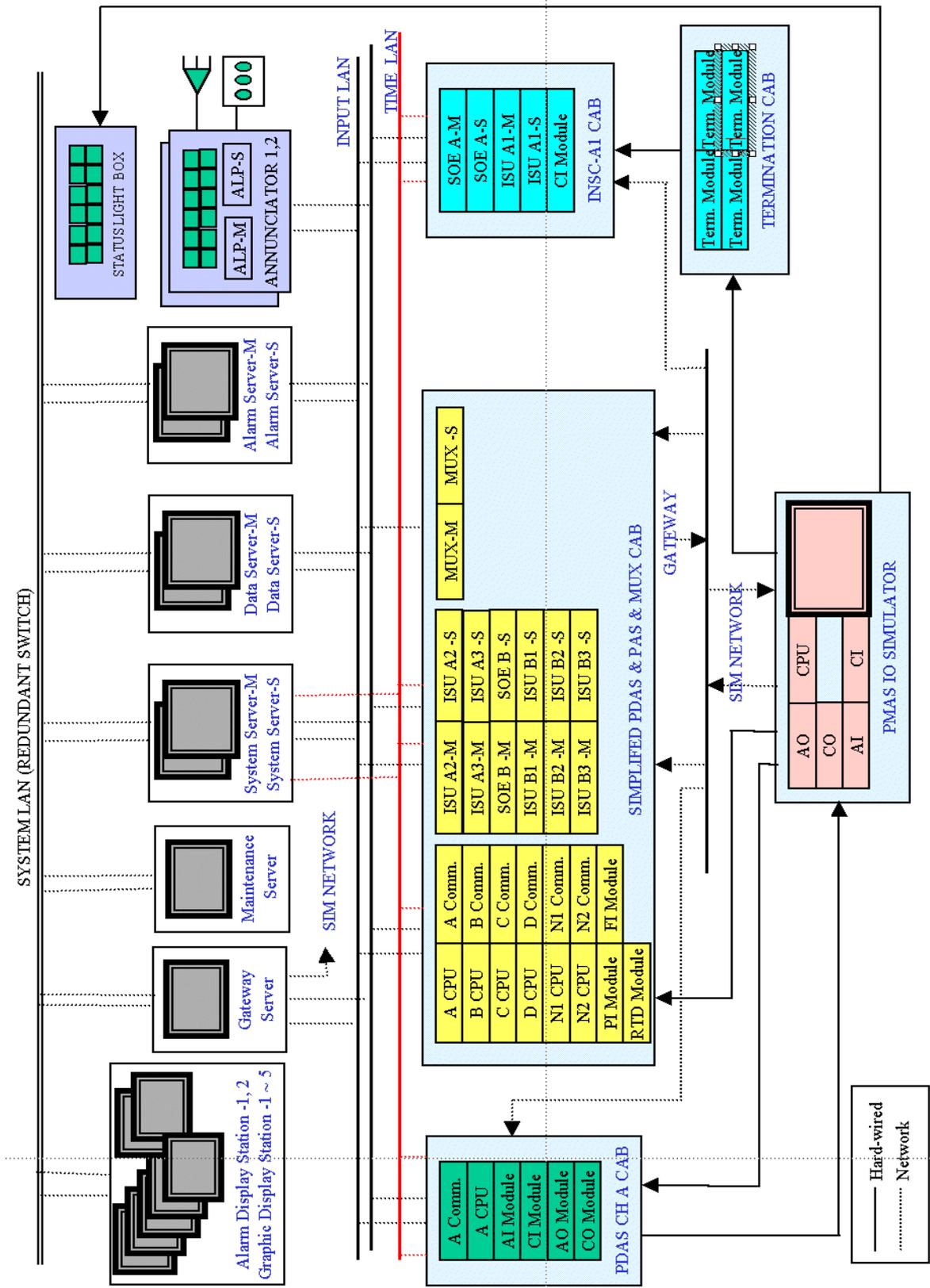


그림 2. 프로토타입 구성도

2.6.1.2 PAS

PAS 는 안전(Isolation Cabinet A, B, C, D) 및 비안전(Input Scanner, Termination, Remote Mux. Cabinet 및 주제어실에 설치된 경보에 필요한 구성기기) 장비로 구성되지만, 프로토타입에서는 Input Scanner(INSC) Cabinet A1 만 실제와 같이 Full Scope 으로 구현하고 다른 캐비닛들은 CPU 카드 및 관련 부품들로 입력신호를 모사하여 PAS 의 기능을 수행하도록 설계하였다. 또한 PAS 의 모든 프로세싱 유닛들은 Master/Slave 로 이중으로 구성하여 이용률 및 신뢰성이 증대 되도록 구성하였다. INSC 캐비닛은 SOE 프로세싱 유닛과 일반 프로세싱 유닛으로 구성되며, 각 프로세싱 유닛은 CPU, 디지털입력 모듈 및 네트워크장치로 구성되어 경보관련 정보를 처리하여 경보서버와 경보창의 경보논리프로세서(Alarm Logic Processor; ALP)에 전달한다. 경보창은 경보타일, 램프, ALP, 청각장치 및 제어 푸쉬버튼들로 구성되어 경보 논리를 처리하고 인간-기계 연계를 제공한다.

2.6.1.3 I/O Simulator

I/O Simulator 는 신호처리 모듈, 아날로그 및 Digital I/O 모듈, CPU 및 네트워크 모듈들로 구성되어 아날로그 및 디지털 입력신호를 실 배선으로 PDAS 및 PAS 에 제공하고, Simulator 에서 모사한 신호를 네트워크를 통해 각 기능을 구현하고 있는 CPU 들에 제공한다. 또한 I/O Simulator 는 PDAS 로부터 출력신호를 받아서 CRT 에 기록계 및 지시계 형태로 표시하여 기능의 적절성 여부를 판단할 수 있도록 하였다.

2.6.1.4 PCS

PCS 는 산업용 컴퓨터를 이용하여 시스템서버, 데이터서버, 경보서버, 유지보수용서버, 게이트웨이 및 디스플레이 스테이션들로 구성되어 PDAS 및 PAS 로부터 데이터를 입력받아 처리하고 CRT 및 프린터로 자료를 표시하고 인쇄해 준다. PCS 는 Master/Slave 형태의 구성을 가지며 어느 한 프로세서의 고장 또는 어느 한 네트워크의 고장시 자동적인 전환(Failover)을 감지하여 계속해서 고유의 기능을 수행할 수 있도록 이중으로 구성되어 이용률 및 신뢰성을 증대 시키도록 설계하였다. 정상운전동안에는 Master 가 온라인 Active 이고 Slave 는 Hot Standby 상태가 되어 Master 와 같은 기능을 수행하지만 결과를 출력하지는 않는다.

2.6.1.5 네트워크

PMAS 프로토타입의 네트워크는 Input LAN, System LAN, Time LAN 및 Simulation LAN 들로 구성된다. System LAN 은 TCP/IP 또는 UDP/IP 프로토콜을 지원하는 100 Mbps Switched Ethernet 이며 PCS 의 각 서버들, MMI 장치들 및 게이트웨이와의 연계를 담당한다. Input LAN 은 TCP/IP 또는 UDP/IP 프로토콜을 지원하며 PDAS 및 PAS 의 각 캐비닛, PAS 의 각 경보창 및 PCS 의 각 서버들과의 연계를 담당한다. Time LAN 은 시각 동기를 유지하기 위한 네트워크이며, GPS 로부터 시각 정보를 받아서 대한민국 표준시간으로 바꾸어 각 캐비닛의 시각을 동기화시키는 역할을 한다. Simulation LAN 은 100 Mbps Ethernet 이며 I/O Simulator 에서 모사된 데이터를 PDAS 및 PAS 로 전송하고, 게이트웨이를 경유하여 PCS 의 각 서버에서 계산된 값들을 받는 경로를 담당한다.

2.6.2 소프트웨어

PMAS 프로토타입에서 개발되는 소프트웨어는 신규호기에 새로운 시스템 구성 및 운영 체제를 적용할 때 상대적으로 개발 시간이 많이 소요되는 시스템 소프트웨어, 통신 소프트웨어

어, MMI 소프트웨어, 그리고 기존의 CFMS 를 개선한 SPADES 등 사전 성능확인이 필요한 일부 NSSS 응용프로그램 등이 포함된다. 또한 이들 소프트웨어는 신규호기 적용 전에 설계 변경에 따른 영향 평가 및 성능 검증을 위해 실제 프로젝트와 동일한 수준의 품질 활동을 수행하였다.

2.6.2.1 개발 방향

- 국내 경수로의 정보계통에 모두 적용 가능한 소프트웨어 설계
- 중앙 집중형 및 분산형 시스템 구성을 모두 지원할 수 있는 소프트웨어 설계
- 소프트웨어 유지 보수시, 소스코드 수준의 변경 없이 MMI 상에서 설정 변경만으로 수용 가능하도록 설계
- 실시간 운영체제 하에서 정확한 태스크 스케줄링이 가능하도록 설계
- POSIX 호환 코드로 작성하여 소프트웨어 이식성이 높도록 설계

2.6.2.2 주요 소프트웨어 모듈

- 시스템 소프트웨어
 - Failover
 - Input/Output Processing
 - Task Scheduling
 - Database
- 통신 소프트웨어
 - NSSS and BOP Systems Communication
 - Internal Communication (PDAS, PAS, PCS)
 - Plant LAN Communication
- MMI 소프트웨어
 - Operator Monitoring
 - Operator Support, Maintenance and Operation
 - Display Processing
 - Alarm Processing
 - Log and Report Processing
- NSSS 응용프로그램
 - SPADES
 - UTDV
 - CEA Application
 - Incore Processing

2.6.2.3 소프트웨어 품질확인(QA)

소프트웨어 품질확보를 위해서 수행된 주요작업은 다음과 같다.

- 소프트웨어 개발 관리
소프트웨어 설계지침서 및 MMI 설계지침서에 따라 소프트웨어 개발
- 소프트웨어 형상관리
소프트웨어 형상관리 절차서에 따라 관리
- 소프트웨어 확인 및 검증

- 소프트웨어 확인 및 검증 계획서에 따라 확인 및 검증 업무 수행
- 소프트웨어 시험
 - 소프트웨어 단위시험, 시스템 통합시험, 공장시험, 현장인수시험 등 수행
- 소프트웨어 품질 관련 문서화
 - 소프트웨어 품질 향상을 위해 각 수명주기 단계별로 요구되는 설계요건서, 설계서, 시험 절차서, 시험보고서, 사용자 문서 등 작성

3. 결 론

본 논문에서는 표준원전의 발전소감시계통과 경보계통을 통합설계하기 위한 관련 규제요건과 기술사항 등을 고찰하였다. 또한 본과제의 일환으로 실제 건설공정에서 인간공학적 설계 및 평가업무 수행을 위하여 HFEP 및 HFE V&V Plan 을 작성하였다. 통합설계에 따른 기대효과는 다음과 같이 결론 지을 수 있다.

- PMS 와 PAS 의 경보와 표시방법의 일관성 있는 설계에 따른 인간공학적 측면에서의 향상
- 유사기능을 통합함으로써 설계 단순화 추구
- 중복신호 제거에 따른 경제성 향상
- 개방형 시스템을 사용함에 따른 이식성 향상
- 운전원 중심의 MMI 를 제공함에 따른 이용률 증대
- 경보기능 및 운전원 지원기능 강화
- PMS 와 PAS 에 동일 부품 혹은 유사부품을 사용함에 따른 유지보수성 강화

본 통합설계를 통하여 기존에 외국 설계 기술과 제품에 의존하던 것을 탈피하여 설계 및 제품개발의 완전 국산화가 가능할 것으로 판단된다. 또한, 신규원전 1,2 호기에 본 설계결과를 직접 적용하기 전에 프로토타입을 제작하여 통합설계에 대한 구현성을 검증함으로써 보다 안정된 설계와 제품을 적기에 제공할 수 있을 것이다.

참 고 문 헌

- 1) NUREG-0800, "Chapter 7. Instrumentation and Controls", USNRC, Rev.04, June 1997.
- 2) 경수로형원전 안전심사지침, "제 18 장 인간공학", 한국원자력안전기술원, 개정 2 판, 1999.
- 3) SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs", USNRC, April 1993.
- 4) Memorandum for SECY-93-087, II.T, USNRC, July 1993.
- 5) IEEE-7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", IEEE, 1993.
- 6) RG 1.47, Rev.00, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems", Program Functional Specification, USNRC, May 1973.
- 7) NUREG-0696, "Functional Criteria for Emergency Response Facilities", USNRC, February 1982.
- 8) Advanced Light Water Reactor Utility Requirement Document, Chapter 10, Man-Machine Interface System, December 1995.
- 9) KOPEC/99-TN-9AJ, "비상운전 지원을 위한 필수안전기능 감시계통 개발과제 최종보고서", KOPEC, May 1995.

- 10) 이 순성 외 8인, "발전소감시 및 경보계통에 대한 고찰", 전력기술 통권 제 36 호(제 11 권 제 1 집), KOPEC, 2000.