2000 추계학술발표회 논문집
한국원자력연구소

액금로 원자로보호계통 프로토타입 개발
Development of Prototype for Reactor Protection System in Liquid Metal Reactor

김창회, 천세우

한국원자력연구소
대전광역시 유성구 덕진동 150

요 약

본 논문은 액금로 원자로 보호계통 설계와 설계검증을 위해 개발된 보호계통 프로토타입에 대해 기술한다. 개발된 프로토타입은 개념설계를 통해 개발된 보호계통의 구조에 따라 4-채널 디지털 시스템으로 구성하고, 각 채널은 이중화 CPU, 이중화 이드넷, 이중화 필드버스, 그리고 센서 입력을 받아들이는 아날로그 입력단, 트립 결과를 트립 브레이크로 전송하는 출력단 등 상용 PLC를 사용하여 구성한다. 각 채널 캐비넷에는 경보창 패널, 전체 미믹 패널, 바이패스 및 테스트 패널 등을 설치하여 운전원이 수동 조작 및 상태를 감시할 수 있도록 한다. 개발된 하드웨어 구조와 소프트웨어 트립 로직의 타당성을 검증하기 위해 시험환경을 구축한 후 시험 시나리오에 따라 모의시험을 수행한다.

Abstract

This paper describes the prototype for liquid metal reactor protection system. The prototype is configured of the four channelized digital system based on a commercial PLC according to design criteria and conceptual design. Each channel consists of several PLC modules such as redundant CPU, analog and digital I/O, redundant Ethernet, redundant optical fieldbus, and power supply. The cabinet panel in each channel consists of the annunciator, overall mimic, and test and bypass panels. To evaluate the performance of the software trip algorithm and redundant hardware module, several simulations with different scenarios have been done using the RPS prototype.

1. 서 론

기존의 원자로 보호계통은 오래된 아날로그 기술을 사용하고 있어 유지보수나 재고품 확보 등이 어려워 최근에는 디지털 보호계통을 사용하는 발전소가 늘어나고 있다. 디지털 보호계통은 기존 아날로그에 비해 유연성, 정확도, 유지보수성, 공간확보의 용이성, 지능형 온-라인 모니터링 및 진단기법의 적용 등과 같은 장점을 갖고 있다.

액금로 원자로보호계통의 주 기능은 원자로 보호변수가 안전 설정치를 초과할 경우 원자로를 자동으로 정지시키는 기능을 수행한다. 또한, 기존 PWR 원자로와는 달리 액금로는 소듐(액체 나

트륨)을 냉각재로 사용하기 때문에 2차측의 물과 1차측의 소듐이 반응하여 폭발하는 것을 방지하기 위해 중간 열전송계통(IHTS: Intermediate Heat Transfer System) 내의 압력이 안전 설정치를 초과할 경우 원자로 보호계통은 자동으로 IHTS 격리밸브를 닫아서 IHX(Intermediate Heater Exchanger)를 보호하는 기능을 수행한다.

본 논문에서는 액금로 원자로 보호계통 설계와 설계검증을 위해 개발한 보호계통 프로토타입에 대해 기술하였다. 보호계통 프로토타입은 개념설계를 통해 개발된 보호계통의 구성의 타당성 및 실현 가능성에 대한 검증, 소프트웨어 트립 로직의 개발 및 구현을 통한 검증, 개발된 요건(시험성 및 실시간 요건 등)을 만족시키기 위한 방안 마련 및 요건의 재정립 등을 확인, 검증하기 위해 개발하였다. 이러한 이유로 개념설계 단계에서 개발된 보호계통의 구조와 가능한 유사한 구성을 갖도록 하였고, 차후 수정보완이 용이하도록 유연성을 갖는 구조를 선택하여 개발하였다.

개발된 프로토타입은 이중화 CPU, 이중화 이드넷, 이중화 필드버스, 그리고 센서 입력을 받아들이는 아날로그 입력단, 트립 결과를 트립 브레이크로 전송하는 출력단 등 상용 PLC를 사용하여 구성하였으며, 구성된 PLC를 4개의 채널로 나누어진 캐비넷내에 설치하였다. 또한, 운전원의 수동 조작과 상태 감시를 위해 캐비넷 전면부는 경보창 패널, 전체 미믹 패널, 바이패스 및 테스트 패널 등을 구성하여 설치하였다. 또한, 디지털 보호계통의 소프트웨어 트립 로직의 개발과 구현 가능성을 확인하기 위해 바이스테이블 로직과 동시논리를 개발하여 프로토타입에 실장하였고, 운전원 화면을 개발하여 프로토타입과 연계하였다. 개발된 하드웨어 구조와 소프트웨어 트립 로직의 타당성을 검증하기 위해 시험환경을 구축한 후 시험 시나리오에 따라 모의시험을 수행하였다. 시험환경은 안전변수를 발생시키는 코드 시뮬레이터와 그 결과를 이드넷으로 전송받아서 현장의 안전 센서신호로 변환해주는 VXI 시스템, 프로토타입, 그리고 운전원 화면 등으로 구성된다.

2. 액금로 원자로보호계통 개념 설계

액금로 원자로보호계통은 설계기준사고 발생시 발전소 안전을 위해 원자로를 자동으로 정지시키는데 필요한 기능을 수행한다. 따라서, 원자로보호계통은 원자로를 보호하기 위해 안전변수가 정해진 설정치를 초과할 경우 제어봉을 노내에 삽입하여 원자로를 정지시키고, 소듐유입으로 인한 압력상승으로부터 IHX(Intermediate Heater Exchanger)를 보호하기 위해 ITHS(Intermediat Heat Transfer System) 격리밸브를 자동으로 차단하는 기능을 수행한다. 또한, 원자로 정지시 주냉각제 펌프(EM pump)를 정지시키는 펌프 정지계통과 연계하여 주냉각재 유량을 단속시키는 기능을 수행한다. 액금로 원자로 보호계통에 사용되는 안전 정지변수로는 중성자속, 주 냉각재 유량, 원자로 풀의 소듐 수위, 노심 입구 및 출구측 온도, IHTS 압력, 격납용기 방사능 준위, 수동정지 등이 있다. 원자로 보호계통은 주 냉각재 펌프 정지계통과 연계하고, 주제어실의 제어반, 원격정지반(Remote Shutdown Panel), IEEE Class 1E PAM(Post Accident Monitoring) 센서신호와 연계된다. 그림 1은 원자로 보호계통에 의해 작동되는 세부계통과의 연계를 나타낸다.

2.1 액금로 보호계통 설계개념 및 요건

액금로 보호계통 개발을 위해 설정된 설계개념은 크게 단일고장 및 공통모드고장에 대한 대비, 통신망 기반의 4-채널 디지털시스템의 적용, 그리고 시험기능의 향상으로 요약된다. 따라서, 액금로 보호계통은 4-채널로 구성된 디지털시스템으로 개발하고, 각 채널간은 물리적/전기적으로 격리하여 채널 독립성을 유지하도록 한다. 이것은 어떤 채널내에서 발생한 단일고장이 타 채널로 전파되어 전체 보호기능이 상실되지 않도록 하기 위함이다.

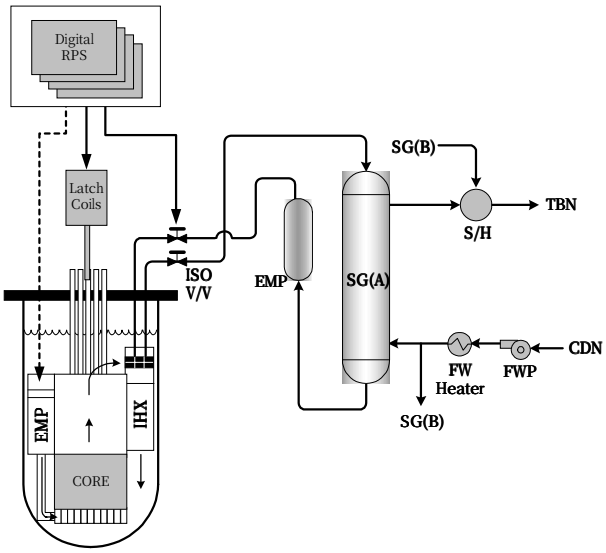


그림 1. 원자로 보호계통에 의한 세부 작동계통

보호계통에 사용되는 트립 로직은 2/4 소프트웨어 보팅 로직을 사용하고, 어떤 채널의 고장시 자동으로 2/3 로직으로 자동 재구성되도록 한다. 확대된 데이터 통신을 보호계통에 적용하기 위해 각 채널간, 원격정지반, 제어실, 그리고 비안전제어계통 등과의 데이터 전송에 서로 다른 특성을 갖는 데이터 네트워크를 사용한다. 그리고, 적용된 각 데이터 링크는 가능한 이중화구조를 채택하여 신뢰도를 향상시키고, 광소자 등을 사용하여 전기적 격리가 이루어지도록 한다. 보호계통의 각 채널에 사용되는 하드웨어 모듈들은 유지보수성 향상을 위해 표준화된 모듈을 사용하고, 신뢰도 및 단일고장 방지를 위해 고장허용구조를 갖도록 한다. 보호계통에 적용되는 모든 소프트웨어는 안전 소프트웨어 품질보증 요건을 확대 적용하여 안전등급 소프트웨어 기준을 만족하도록 한다.

보호계통 하드웨어 시험 및 기능 시험성을 향상시키기 위해 자동주기시험 및 자가진단기능을 적용한다. 자동주기 기능시험은 센서 입력단에서부터 트립 브레이크단까지 모든 하드웨어 및 소프트웨어에 대한 기능을 시험할 수 있도록 하고, 이 시험으로 인해 보호계통 동작이 방해받지 않도록 한다. 이 시험은 수동으로 개시되고 자동으로 진행되도록 한다. 자가진단은 보호계통의 하드웨어 고장을 감지하기 위해 연속적으로 수행되며, 고장 검출시 이를 배제한 후 자동으로 재구성되도록 하여 운전성을 향상시킨다.

이러한 설계개념을 만족시키기 위해 한국의 규제요건[1,2], GDC(General Design Criterion)[4], Regulatory Guides[5,6], NUREG Guides[7], 그리고 ANSI/IEEE Standards[8,9,10] 등을 참조하여 성능요건, 기능요건, 그리고 설계요건을 개발하였다[11].

2.2 보호계통 개념설계

액금로 보호계통 설계개념과 설계요건에 따라 4-채널 디지털 보호계통 구조를 설정하였다. 각 채널은 입출력 모듈, 바이스테이블 모듈, 동시논리모듈, 그리고 기능적으로 분리된 3개의 데이터 네트워크 모듈로 구성된다.

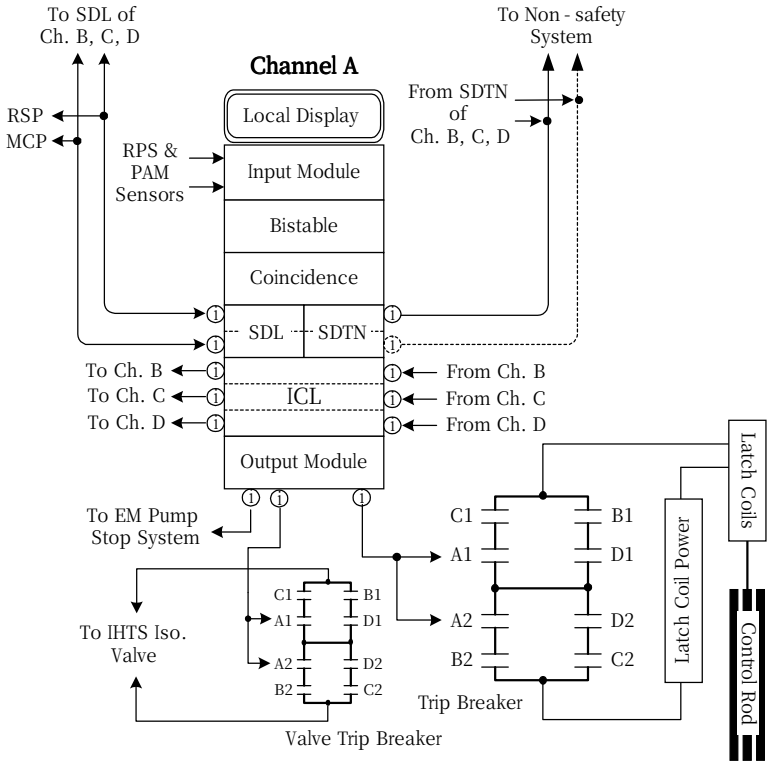


그림 2. 액금로 보호계통의 하드웨어 구조

입력모듈은 안전 센서신호와 PAM 신호를 취득한 후 디지털로 변환한다. 센서고장을 검출하기 위해 취득된 센서신호는 정해진 제한치(하한치 및 상한치)와 연속적으로 비교되고, 신호가 제한치를 초과할 경우 고장으로 판단되어 운전원에 의해 채널 트립 바이패스가 수행된다.

바이스테이블 모듈은 히스테리시스를 갖는 고정설정치와 가변설정치를 실시간으로 계산한 후 입력모듈에서 전송된 센서신호와 이들 설정치를 비교하여 트립 혹은 프리-트립(Pre-trip) 신호를 발생시킨다. 또한, 이 모듈은 원자로 기동 및 정지운전시 또는 저출력 시험시 불필요한 트립이 발생되는 것을 방지하기 위한 운전우회기능을 갖는다. 운전우회기능은 측정된 안전변수가 운전우회 허용 범위내에 있고, 운전원이 운전우회를 요구할 경우 바이스테이블의 트립 또는 프리-트립 결과가 자동으로 리셋된다. 이 기능은 수동으로 개시되고 발전소 조건이 운전우회범위를 벗어날 경우 자동으로 제거된다. 따라서, 이 모듈에는 설정치 계산블록, 비교연산블록, 운전우회 연산블록 등이 포함된다.

동시논리모듈은 자기 채널의 바이스테이블의 결과와 다른 3개의 채널에서 전송된 바이스테이블 결과를 사용하여 2/4 보팅로직을 수행한다. 만약, 어떤 하나의 채널이 고장 또는 시험으로 기능을 수행하지 못할 때 2/4 로직은 자동으로 2/3 로직으로 재구성된다. 따라서, 이 모듈에는 2/4 보팅로직을 연산하는 블록과 채널 트립 바이패스를 연산하는 블록이 포함된다. 채널 트립 바이패스 블록에서는 두 개의 채널이 동시에 바이패스되는 것을 방지하기 위해 first-in-first-out 개념을 사용한다. 이런 이유로 어떤 채널이 이미 트립 채널 바이패스되어 있을 때 또 다른 채널에서 바이패스를 요구하면 그 요구신호는 자동으로 제거된다.

출력모듈에서는 각 동시논리 모듈의 신호를 "OR" 로직으로 조합하여 원자로를 정지하기 위한

트립 브레이크와 IHTS 격리 밸브를 동작시키기 위한 트립 브레이크로 트립신호를 발생시킨다. 이 신호는 전기적 격리를 위해 광소자로 격리된 하드와이어를 통해 전송된다. 또한, 원자로 정지 후 주냉각재 펌프정지를 위해 펌프정지계통으로 원자로 트립신호를 전송한다.

출력모듈과 연계된 트립 브레이크는 그림 2에서처럼 전 2/4 하드와이어 보팅로직으로 구성하였다. 따라서, 브레이크는 각 한 채널당 2개씩 모두 8개로 구성되고, 출력모듈의 신호는 2개의 하드와이어를 통해 이들과 연결된다.

ICL(Inter-Cahnnel Link)은 보호계통내 각 채널간에 채널고장상태, 트립 채널 바이패스상태, 그리고 바이스테이블 결과와 같은 특정한 데이터를 전송하기 위해 사용된다. 이 링크는 채널간의 독립성을 유지하기 위해 광케이블을 사용하고, 데이터 전송시간 동기화를 위해 한 채널에서 다른 채널로 단방향으로 데이터를 전송하도록 기능을 제한하였다. 따라서, 각 채널내에는 송신부와 수신부가 분리되어 있다.

SDL(Safety Data Link)는 보호계통의 정보를 주제어실 제어반과 원격정지반에서 서로 공유하기 위해 사용된다. 이 링크 또한 독립성 유지를 위해 보호계통과 주제어실 제어반 그리고 보호계통과 원격 정지반을 연결하는 전송라인을 서로 다르게 사용하도록 설계하였다.

SDTN(Safety Data Transmission Network)은 보호계통의 정보를 비안전 제어계통 등으로 전송하기 위해 사용된다. 따라서, 이 네트워크는 보호계통에서 단방향으로 정보가 전송되고, 비안전급(Non-class 1E)으로 분류된다.

그림 3은 보호계통과 타계통과의 연계를 나타낸다. 원자로 수동정지 및 격리밸브 수동차단은 주제어실과 원격 정지반에서 수행할 수 있고, 이 신호는 하드와이어를 통해 브레이크와 직접 연결된다.

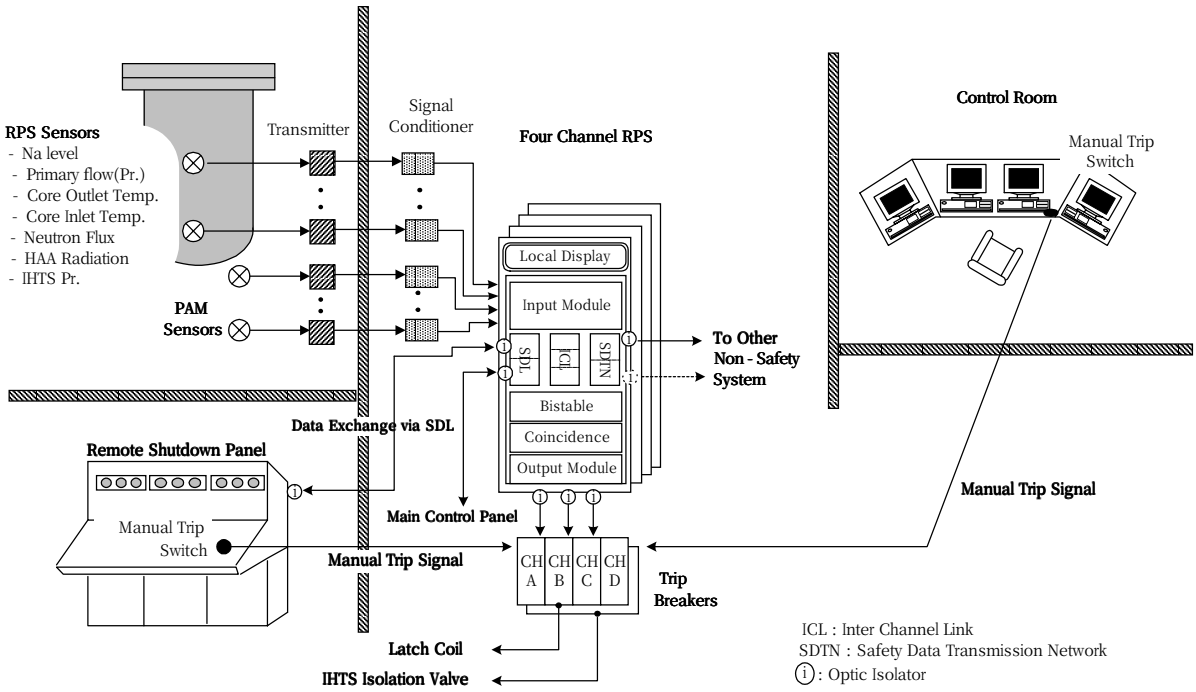


그림 3. 보호계통과 타계통과의 연계

3. 보호계통 프로토타입 개발

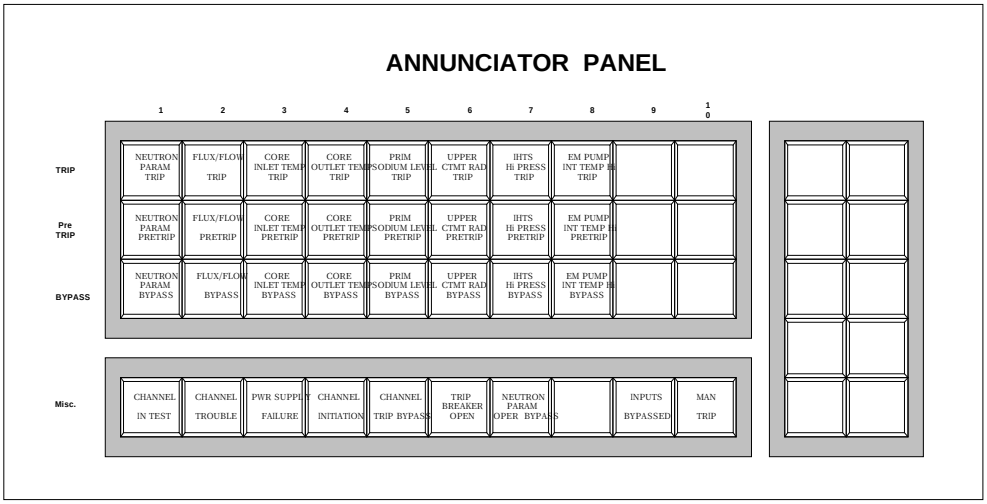
개념설계를 통해 개발된 보호계통의 구성의 타당성과 실현 가능성에 대한 검증, 소프트웨어 트립 로직의 개발 및 구현을 통한 검증, 개발된 요건(시험성 및 실시간 요건 등)을 만족시키기 위한 방안 마련 및 요건의 재정립 등을 확인, 검증하기 위해 보호계통 프로토타입을 개발하였다. 이러한 이유로 개념설계 단계에서 개발된 보호계통의 구조와 가능한 유사한 구성을 갖도록 하였고, 차후 수정보완이 용이하도록 유연성을 갖는 구조를 선택하여 개발하였다.

3.1 프로토타입 하드웨어

개발된 프로토타입은 상용 PLC를 사용하여 4-채널로 구성하였다. 각 채널에는 바이스테이블 및 동시논리 기능을 수행하는 이중화 CPU, 안전 센서 및 PAM 센서 신호를 받아들이는 기능을 수행하는 입력단, SDL 또는 SDTN 기능을 수행하는 이중화 이드넷 통신, ICL 기능을 수행하는 이중화 필드버스 링크, 그리고 출력단 및 전원단 등으로 구성된다. 이 PLC는 4개의 채널로 구성된 각 캐비넷속에 설치되어 외부 신호와 연계된다. PLC가 내장된 각 캐비넷은 그림 4와 같다. 각 캐비넷 전면부는 경보창(annunciator) 패널, 전체 미믹(overall mimic) 패널, 바이패스 및 테스트 패널 등으로 구성하였다. 그리고 캐비넷내에는 그림에서처럼 PLC와 터미널 블록, 그리고 전원장치, 광케이블 전송기 등이 설치되어 있다.

그림 4. 4-채널로 구성된 보호계통 프로토타입 캐비넷 전면부 및 후면부

경보창 패널에는 각 안전변수의 트립, 프리트립, 그리고 바이패스 상태를 표시하는 창이 있다. 또한, 이 패널에는 전원장치의 고장상태, 채널의 시험, 트립 브레이크의 상태, 운전우회허용 변수에 대한 바이패스 상태, 채널 트립 바이패스 오류 등을 나타내는 창이 설치되어 있다. 따라서, 운전원은 이 패널을 통해 각 채널의 모든 상태를 감시할 수 있다. 그림 5는 경보창 패널의 구성을 나타낸다.



경보 5. 경보창 패널의 구성

전체 미믹 패널은 각 안전변수에 대한 상태와 채널의 운전결과를 전반적으로 보여준다. 따라서, 이 패널에는 안전변수가 현재 어떤 상태로 운전 중인지를 나타내는 상태 램프가 설치되어 있다. 안전 센서의 고장상태, 바이스테이블 결과를 나타내는 프리-트립, 트립 상태, 바이패스 상태, 동시논리 결과 상태, "OR" 조합 로직 상태, 그리고 출력단의 상태를 나타내는 램프들이 시리얼로 표시되도록 배치하여 운전원이 쉽게 각 안전변수의 상태를 확인할 수 있도록 하였다. 또한, 출력단에 의해 트립 브레이크가 정상적으로 동작했는지를 나타내는 트립 브레이크 상태 표시창, 그리고 트립 브레이크에 의해 작동된 주냉각재 펌프, 격리밸브, 원자로 정지를 나타내는 램프가 있고, 이들을 복귀할 때 사용하는 리셋 스위치가 설치되어 있다. 캐비넷내에 설치된 PLC의 CPU 상태나 통신모듈들의 상태, 백업 밧데리의 상태를 나타내는 램프를 설치하여 운전원이 쉽게 PLC의 동작상태를 점검할 수 있도록 하였다. 그림 6은 전체 미믹 패널의 구성을 나타낸다.

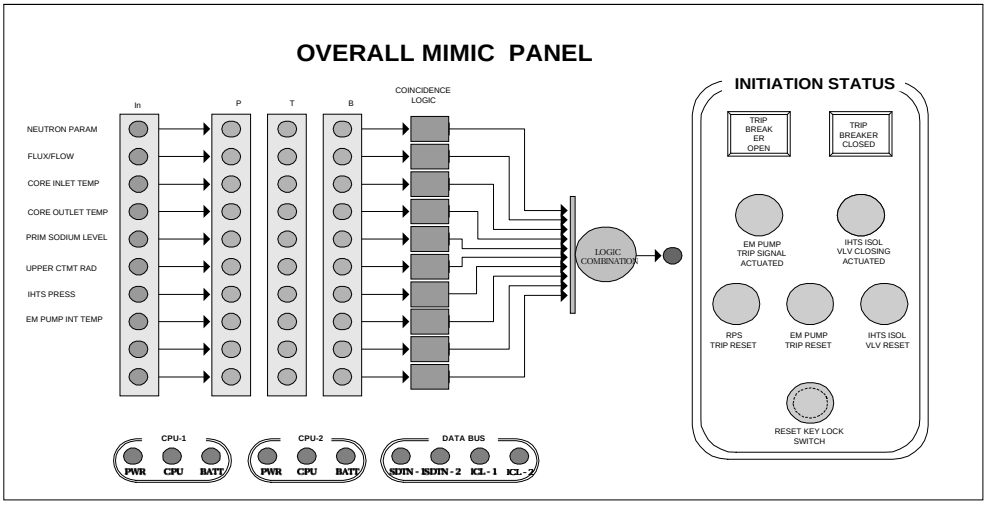


그림 6. 전체 미믹 패널의 구성

바이패스 및 테스트 패널은 자동 또는 수동 주기시험을 수행하고, 채널 바이패스나 운전 바이패스를 수행할 때 사용하는 패널이다. 따라서, 이 패널에는 각 안전변수를 수동으로 바이패스시키는 트립 채널 바이패스 스위치와 운전 바이패스 허용변수를 바이패스하는 스위치 및 복귀 스위가 있다. 트립 채널 바이패스 스위치는 채널 전체를 바이패스시키는 스위치(Inputs Bypass)와 안전변수마다 각각 바아패스시키는 스위치가 각각 설치되어 있다. 채널 전체를 바이패스시킬 때에는 안전을 위해 먼저 "Key Lock" 스위치를 돌린 후 "Inputs Bypass" 스위치를 동작시키도록 설계하였다. 그리고 각 입력 채널에 대해 수동 시험을 수행하는 스위치와 자동 시험 스위치가 각각 설치되어 있다. 그림 7은 바이패스 및 테스트 패널의 구성을 나타낸다.

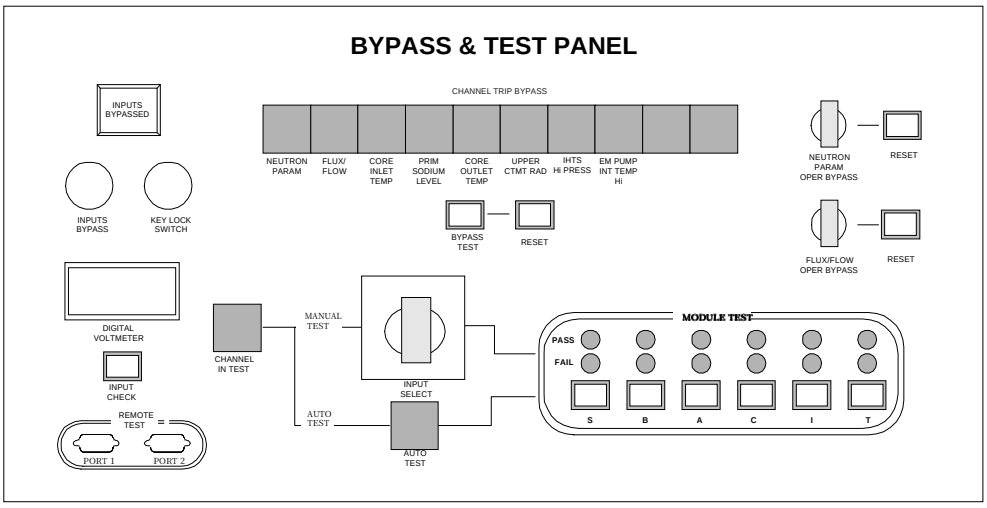


그림 7. 바이패스 및 테스트 패널의 구성

3.2 트립 로직 개발

디지털 보호계통의 소프트웨어 트립 로직의 개발과 구현가능성을 확인하기 위해 바이스테이블 로직과 동시논리를 개발하여 프로토타입에 실장하였다.

구현된 바이스테이블 로직은 그림 8과 같다. 아날로그 입력모듈을 통해 취득된 안전 센서신호는 디지털 값으로 변환된 후 비교 알고리즘을 통해 트립 설정치와 비교되어 프리-트립 또는 트립 신호(로직 레벨 트립)을 발생시킨다. 프리-트립의 경우는 단지 캐비넷 전면부에 설치된 경보창 패널, 전체 미믹 패널, 그리고 운전원 화면에만 표시되도록 하여 운전원이 관심을 가지도록 하였다. 로직 레벨 트립인 경우는 동시논리에서 2/4 보팅 논리를 거쳐 이를 만족하면 원자로 트립으로 진행된다. 이들 프리-트립과 트립 신호는 모두 ICL을 모의한 필드버스 링크를 통해 다른 채널로 전송된다. 트립 설정치 계산 알고리즘은 히스테리시스를 갖는 고정 설정치와 가변 설정치를 실시간으로 계산한다. 프로토타입에서는 안전 정지변수중 중성자속은 가변설정치를 나머지 변수는 고정 설정치와 비교된다고 가정하였다. 또한, 바이스테이블 로직에는 저출력 운전시 불필요한 트립을 방지하기 위해 운전우회기능이 포함되어 있다. 프로토타입에서는 중성자속이 운전우회 허용범위내에 있을 때 운전원이 바이패스 및 테스트 패널에서 수동으로 우회를 요구하면 바이스테이블의 출력 결과가 자동으로 리셋되도록 설계하였다.

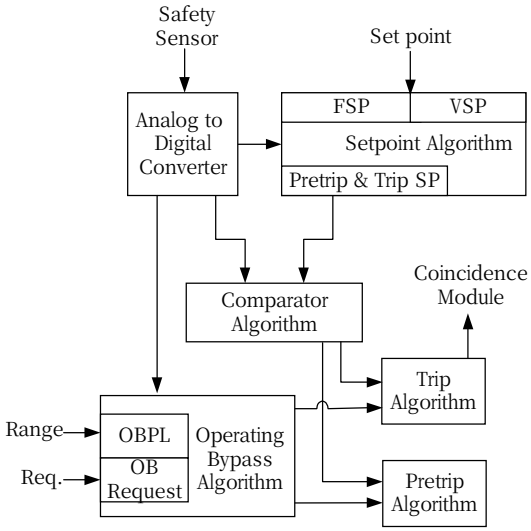


그림 8. 프로토타입 바이스테이블 로직 블록

동시논리는 필드버스를 통해 전송된 각 채널들의 바이스테이블 결과를 받아들여 2/4 보팅로직을 수행하여 그 결과가 "TRUE" 이면 로컬 트립을 발생시킨다. 구현된 동시논리는 그림 9와 같다.

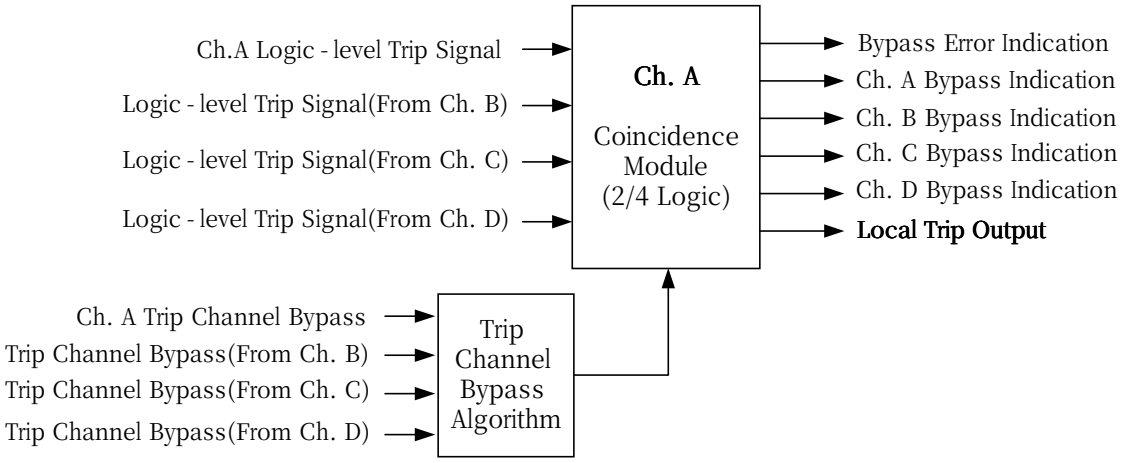


그림 9. 프로토타입 동시논리 블록

동시논리의 결과는 경보창 패널, 전체 미믹 패널, 그리고 운전원 화면에 표시된다. 또한, 동시논리는 고장허용 및 이용율을 높이기 위해 트립 채널 바이패스 신호를 받아들인다. 만약 어떤 안전센서에 고장이 발생했을 경우나 채널을 시험할 경우 운전원이 바이패스 스위치를 동작시키면, 그 신호는 필드버스를 통해 각 채널의 동시논리로 전송되고, 각 채널의 동시논리는 자동으로 2/3 보팅로직으로 재구성한다. 그리고 2개의 채널(채널 A와 B와 같은)에서 동시에 트립 채널 바이패스를 요구할 경우 먼저 요구한 채널만 바이패스되도록 설계하였다. 이것은 2개의 채널이 동시에

바이패스되면 동시논리는 2/2 로직이 되어 항상 로컬 트립이 발생하게 되므로 이를 방지하기 위함이다. 따라서 트립 채널 바이패스 알고리즘에서는 가장 먼저 요구된 채널에 대해서만 바이패스 우선권을 주는 "first-in-first-out" 알고리즘이 포함되어 있다. 만약 운전원이 두 개의 채널을 동시에 바이패스시킬 경우나 한 채널이 바이패스되어 있을 때 또 다른 채널을 바이패스할 경우 바이패스 오류 신호가 각 채널의 경보창 패널에 표시되도록 설계하였다.

각 안전변수에 대한 동시논리의 결과는 "OR" 로직 조합에 의해 트립신호가 만들어지고, 그 결과는 출력단을 거쳐 트립 브레이크로 연결되도록 설계하였다.

3.3 운전 화면개발

보호계통 프로토타입에는 SDL 기능을 수행하는 이드넷 통신모듈이 설치되어 있다. 4개의 채널에 설치된 이중화 이드넷 통신모듈은 허브를 거쳐 운전원 화면을 구동하는 컴퓨터와 연계되어 있다. 따라서, 운전원 화면은 이드넷을 통해 전송된 보호계통 프로토타입의 정보를 운전원에게 표시해주는 기능을 수행한다.

운전원 화면의 구성은 그림 10과 같은 구조로 개발하였다. 즉, 운전원은 오브뷰 화면에서 보호계통의 관련 정보를 감시하고, 필요할 경우 각 상세화면으로 쉽게 이동하여 상세정보를 볼 수 있도록 화면을 배치하였다. 운전원은 오브뷰 화면에서 특정 채널로 들어가서 패널에 표시되어 있는 정보들을 볼 수 있고, 필요할 경우 각 패널로 쉽게 이동할 수 있도록 채널 버튼을 설정하였다. 또한, 오브뷰 화면에는 트랜드, 경보, 하드웨어 관련 정보 화면 등으로 접근하기 위한 버튼을 설정하여 각 안전변수에 대한 추이, 경보상태, 그리고 PLC 내부 하드웨어의 고장상태 화면으로 이동할 수 있도록 설계하였다.

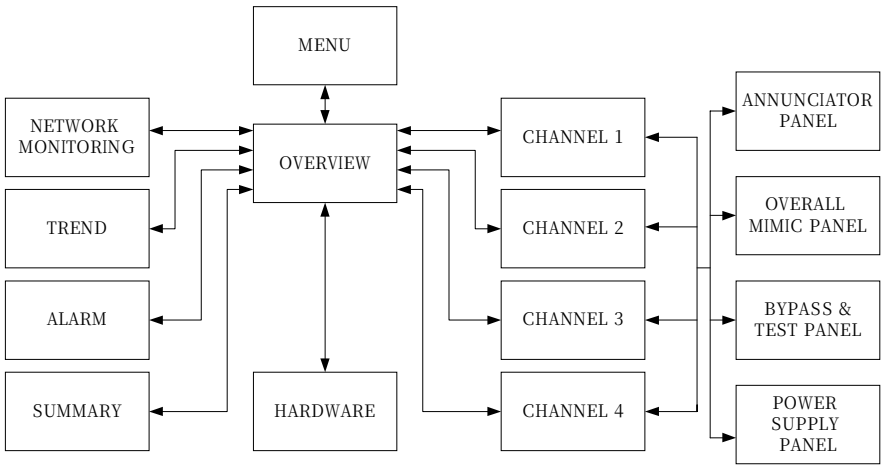


그림 10. 액금로 보호계통 프로토타입 화면 구성도

그림 11은 오브뷰화면을 나타낸다. 운전원이 오브뷰 화면을 통해 1차 계통의 운전 상황을 감시할 수 있도록 하였으며, 경보의 중요도에 따라 다른 색깔로 표시되는 경보창(삼각형 경보표시)을 구성하여 경보 발생 상태를 쉽게 파악할 수 있도록 하였다. 또한, 채널의 각 패널 메뉴 상자를 만들어 항상 패널의 정보를 쉽게 얻을 수 있도록 하였다. 이 화면은 원자로 트립이 발생할 경우 CEDM에 연결된 제어봉이 원자로 속으로 떨어지도록 하였고, 격리밸브 차단 동작이 발생할 경우도

밸브가 잠기는 모양이 에니메이션으로 표시되도록 하여 운전원이나 감시원들이 쉽게 발전소 상황 파악할 수 있도록 하였다. 오브뷰화면은 발전소 운전 상황을 알 수 있는 가장 중요한 화면이기 때문에 다른 화면에서 운전원이 빠르게 오브뷰화면으로 복귀하고자 할 때는 마우스의 오른쪽 버튼을 클릭하면 복귀되도록 설계하였다.

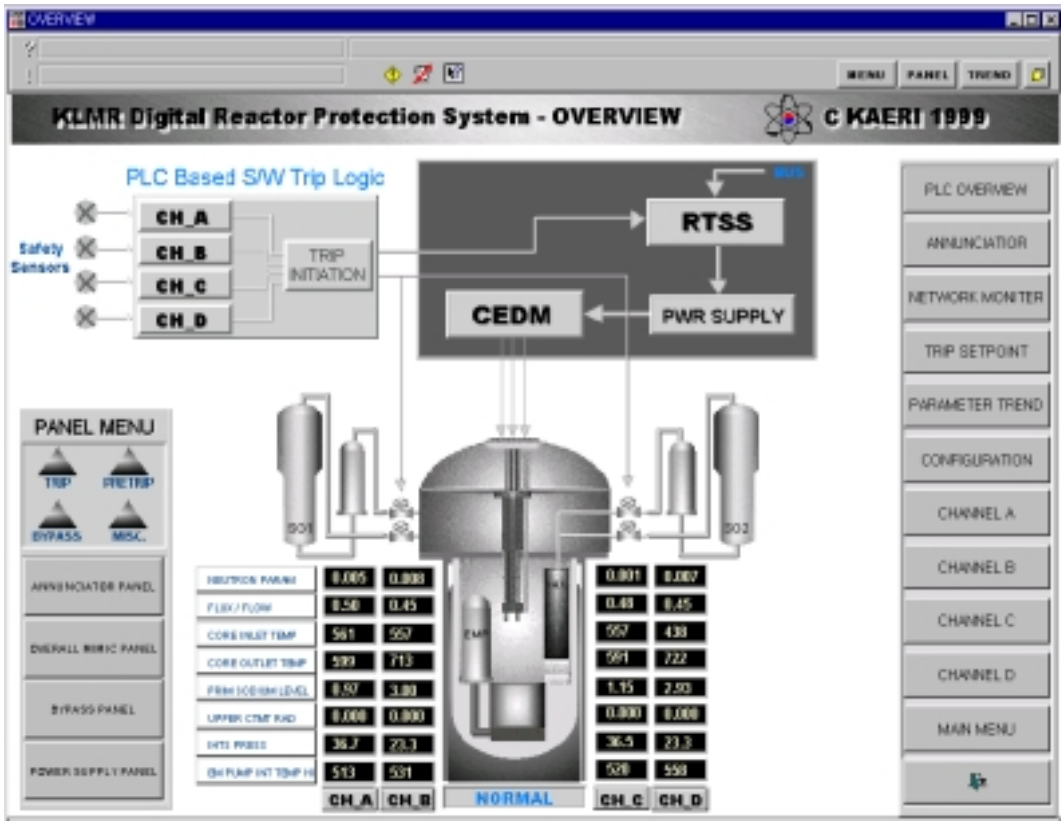


그림 11. 액금로 보호계통 프로토타입 오브뷰 화면

보호계통 프로토타입은 각 채널 당 8개의 안전 변수를 가지며, 이 변수들에 대한 추이를 볼 수 있도록 트랜드 화면을 구성하였다. 트랜드 화면은 각 안전변수만 보여주는 싱글 트랜드 화면, 4개 채널의 특정 변수를 하나의 트랜드 화면에 보여주는 화면, 같은 채널 내에 있는 8개의 변수를 한 화면에 모두 보여주는 트랜드 화면 등으로 구성하였다. 싱글 트랜드 화면에서는 안전변수 트랜드, 트립 및 프리-트립 설정치, 그리고 안전 변수값을 수치로 보여주도록 설계하여 운전원이 현재값과 설정치간의 차이를 쉽게 비교할 수 있도록 구성하였다. 그림 12는 구성된 트랜드 화면을 나타낸다.

보호계통 프로토타입 전면부에 설치된 경보창 패널, 전체 미믹 패널, 바이패스 및 테스트 패널, 그리고 전원 패널에 대한 정보를 운전원이 쉽게 확인할 수 있도록 실제 패널과 유사하게 화면을 구성하였다. 이 화면은 에니메이션 기법을 활용하여 패널의 조작스위치를 누르거나 돌릴 경우 실제처럼 표시되는 것이 특징이다. 그림 13은 구성된 프로토타입 전면부 패널 화면을 나타낸다.

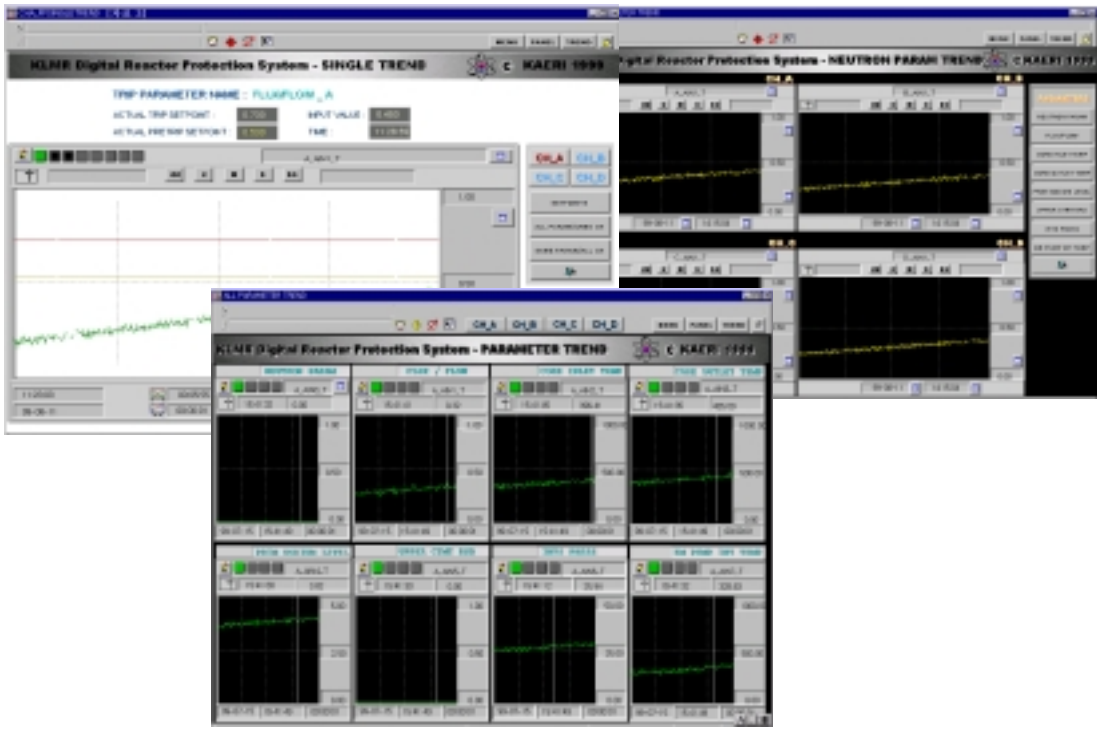


그림 12. 액금로 보호계통 프로토타입 트랜드 화면

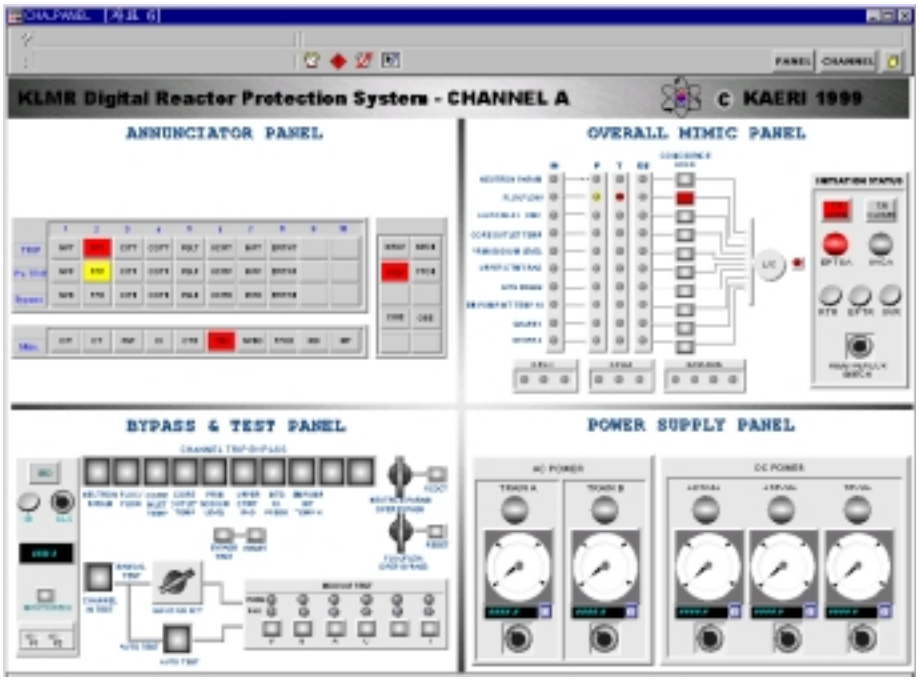


그림 13. 액금로 보호계통 프로토타입 전면부 패널 화면

4. 모의시험 및 검토

개발된 프로토타입 하드웨어와 소프트웨어 트립 로직의 타당성을 검증하기 위해 시험환경을 구축한 후 모의시험을 수행하였다. 모의시험은 하드웨어의 동작성과 소프트웨어 트립 로직의 작동성에 대해 각각 수행하였다.

프로토타입 시험을 위해 원자로 안전변수를 발생시키는 일종의 모의실험장치와 현장의 센서신호 출력을 발생시키는 장치를 구성하여 프로토타입과 연계하였다. 구축된 시험환경은 그림 14와 같다. 코드 시뮬레이터는 워크스테이션을 사용하여 개발하였고, 액금로 동특성을 모의화하여 원자로 운전조건에 따라 프로토타입에서 정의된 안전변수를 엔지니어링 값으로 발생시킨다. VXI(VME-BUS Extended for Instrumentation) 장비는 이드넷을 통해 코드 시뮬레이터와 연계되어 있고, 코드 시뮬레이터에서 발생된 엔지니어링 데이터를 실제 발전소의 안전 센서신호(4~20mA 또는 0~10Vdc)로 변환하는 역할을 수행한다. 프로토타입 입력단은 하드와이어를 통해 VXI의 출력단과 직접 연결되어있기 때문에 VXI를 통해 발생된 현장 센서 신호를 받아들여 디지털로 변환한 후 트립 로직을 수행한다. 운전원 화면은 이중화 이드넷을 통해 프로토타입과 연결되어 있고, 프로토타입의 모든 정보를 받아서 운전원에게 표시해주는 기능을 수행한다. 운전원 화면은 보호계통 요건에 따라 조작행위는 할 수 없고, 단지 정보를 표시하기만 하도록 설계하였다. 이것은 운전원 조작 오류로 인해 원자로가 정지되는 것을 막기 위함이다.

하드웨어의 동작성과 트립 로직에 대한 타당성을 확인, 검증하기 위해 모의시험을 수행하였다. 하드웨어 동작성에 대한 확인 시험은 이중화 CPU의 동작성, 이중화 이드넷의 동작성, 그리고 이중화 필드버스의 동작성에 대한 시험을 수행하였다. 먼저, 이중화 CPU의 동작성을 확인하기 위해 마스터 CPU에 갑자기 고장이 발생하였을 때 슬래브 CPU로 기능 전환이 제대로 이루어지는지를 시험하였다. 시험결과 기능 전환은 제대로 이루어졌지만 전환시 어느 정도 시간이 소요(1초 이내)되었고, 이 시간에 의해 보호계통 동작에 문제가 발생할 것인가에 대해서는 추후 연구가 필요하다는 결론을 도출하였다. 이중화 이드넷의 동작성을 확인하기 위해 한쪽 통신라인에 고장이 발생하였을 때 운전원 화면에 미치는 영향을 살펴보았다. 시험결과 2개의 통신라인으로 병렬로 데이터를 전송하고 있었기 때문에 한쪽 라인에 고장이 발생하여도 운전화면에는 영향을 주지 않는다는 것을 알 수 있었다. 또한, 이중화 필드버스에서 한쪽 통신라인에 고장이 발생하였을 때 채널간의 데이터 전송에 미치는 영향을 분석하였다. 필드버스도 이중화를 사용하여 병렬로 데이터를 전송하기 때문에 고장시 데이터 전송에 문제가 발생하지 않는다는 것을 알 수 있었다. 그러나 데이터 전송 동기화, 즉 채널 B, C, D에서 채널 A로 데이터를 전송할 때 서로 시간적인 동기가 맞지 않아서 생길 수 있는 문제에 대해서는 추후 연구가 필요하다.

소프트웨어 트립 로직에 대한 시험은 다음의 시나리오에 대해 수행하였다.

- 두 개의 채널내에 있는 안전 변수중 어떤 것이 설정치를 초과할 경우 2/4 보팅 로직에 따라 트립이 발생되는지
- 어떤 채널의 안전변수중 어떤 것이 센서 고장으로 인해 트립 채널 바이패스가 되었을 때 2/3 보팅 로직으로 자동 재구성되고, 트립이 발생하지 않는지
- 어떤 채널의 운전우회허용 변수 중 어떤 것이 우회 허용범위내에 있어 수동으로 우회시켰을 때 바이스테이블 결과가 리셋되고, 트립이 발생하지 않는지, 그리고 발전소가 우회조건을 벗어날 경우 자동으로 제거되는지
- 어떤 채널내 안전변수가 트립 채널 바이패스 상태일 때, 다른 채널에서 같은 안전변수에 대해 트립 채널 바이패스를 수행했을 때 바이패스 오류가 발생하고, "first-in-first-out" 알고리즘에 의해 나중에 바이패스한 것이 제거되는지

위의 시나리오에 대해 시험한 결과 개발된 트립 로직이 제대로 동작한다는 것을 확인할 수 있었다. 그러나 안전 소프트웨어 품질보증 요건에 따른 코딩 문제나 확인 및 검증 방법 등에 대해서는 추후 연구가 필요하다는 결론을 도출하였다.

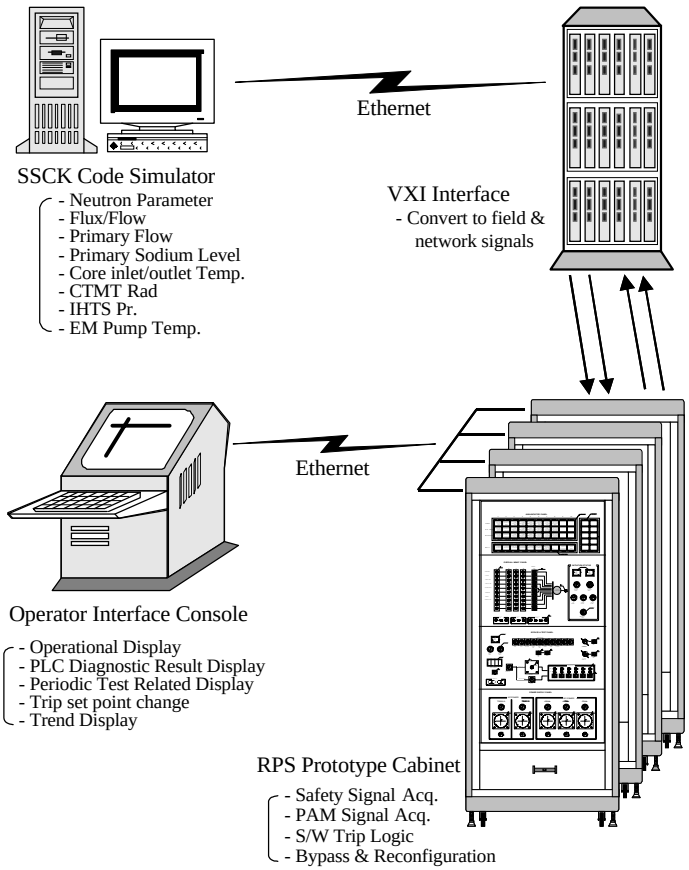


그림 14. 프로토타입 시험 환경

5. 결 론

본 논문은 액금로 원자로 보호계통 설계와 설계검증을 위해 개발된 프로토타입에 대해 기술하였다. 보호계통 설계 개념에 따라 개념설계를 수행하였고, 이를 검증하기 위해 상용 PLC 기반의 4-채널 액금로 보호계통 프로토타입을 개발하였다. 프로토타입은 이중화 CPU, SDL 기능을 수행하는 이중화 이드넷, ICL 기능을 수행하는 이중화 필드버스, 그리고 센서 입력을 받아들이는 아날로그 입력단, 트립 결과를 트립 브레이크로 전송하는 출력단 등으로 구성하여 캐비넷내에 설치하였다. 또한, 운전원의 수동 조작과 상태 감시를 위해 캐비넷 전면부에는 경보창 패널, 전체 미믹 패널, 바이패스 및 테스트 패널 등으로 구성하였다. 디지털 보호계통의 소프트웨어 트립 로직의 개발과 구현가능성을 확인하기 위해 바이스테이블 로직과 동시논리를 개발하여 프로토타입에 실장하였고, 운전원 화면을 개발하여 프로토타입과 연계하였다.

개발된 프로토타입 하드웨어와 소프트웨어 트립로직의 타당성을 검증하기 위해 시험환경을 구

축한 후 모의시험을 수행하였다. 모의시험은 하드웨어의 동작성과 소프트웨어 트립 로직의 작동성에 대해 수행하였고, 시험을 통해 만족할 만한 결과를 얻을 수 있었다.

추후과제로는 개발된 프로토타입을 기반으로 시간 성능요건, 실시간 네트워크 요건, 신뢰성 분석 연구, 이중화 하드웨어에 대한 고장허용 방법론 연구 등을 수행할 예정이고, 단일 고장 및 공통원인 고장에 대한 분석을 수행할 예정이다.

참고문헌

[1] KINS Detailed Safety Section 9.2, Reactor Protection System.

[2] KINS Safety Regulation Guide 9.4, Quality Assurance Guide of Diversity Instrumentation and Control System.

[3] 10 CFR 50.55a(h), Protection System, requires compliance with ANSI/IEEE Std. 279, "Criteria for Protection Systems for Nuclear Power Generating Station".

[4] General Design Criterion 20, Protection System Functions.

[5] Regulatory Guide 1.22. Periodic Testing of Protection System Actuator Functions. Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1972.

[6] Regulatory Guide 1.53. Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems. Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

[7] NUREG-0800, Standard Review Plan: Section 7.0 Instrumentation and Controls, 1997.

[8] IEEE Std. 338-1987, Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems.

[9] IEEE Std. 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

[10] IEEE 7-4.3.2-1993, "IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Station Safety Systems.

[11] Reactor Protection System Design Requirements, LMR/IC132-DR-01/1999, Nov. 1999.

[12] System Description for Plant Protection System for Nuplex 80+, NPX80-IC-SD560, Rev.1, ABB CE, Feb. 1994.