'2000 춘계학술발표회 논문집
한국원자력학회

디지털 플랜트 보호계통 구조 개발

A Development of Digital Plant Protection System Architecture

성승환, 박희윤, 김동훈, 서용석, 구인수
한국원자력연구소

요 약

아날로그 계통에 비해 많은 장점을 가지고 있는 디지털 보호계통은 여러 분야에서 연구되고 있다. 하지만 디지털 계통은 소프트웨어나 프로세서 오류 발생에 매우 취약하다. 이러한 단점을 극복하는 방안으로 한 채널 내에서 세그먼트와 분할 개념을 개발하였다. 세그먼트 개념은 플랜트 과도 상태 발생에 대한 입력 신호의 기능적 다양성에 근거하여 센서 신호로부터 원자로 정지 및 공학적안전설비 개시 신호까지 한 채널 내에서 다시 나누어진다. 분할 개념은 세그먼트 내 각 모듈의 이상 상태를 격리하고 처리하기 위해 각 기능 모듈을 독립적인 프로세싱 모듈로 할당하는 것이다. 그리고 예측가능하고 경성 실시간(hard real time)을 만족하는 결정론적 통신망 프로토콜을 개발하여 각 세그먼트내의 기능 모듈과 채널간의 동시 논리 판단 모듈을 연결하고 있다. 그리고 온라인 시험 기능을 포함하는 자가 진단과 센서부터 개시 신호까지의 기능성을 검사하는 주기적인 시험 기능을 설계하여 보호계통의 안전성, 신뢰성 및 가용성을 높인다. 개발된 보호계통은 산업용으로 널리 이용되는 프로세서인 DSP를 사용하고 또한 VME 버스 구조를 채택하였다. 소프트웨어의 품질 보증 과 확인 및 검증 절차에 대해 개발 중에 있으며 결정론적인 통신망의 구조는 계속 연구중이다.

Abstract

The digital plant protection system(DPPS) which have a large number of advantages

compared to current analog protection system has been developed in various field. The major disadvantages of digital system are, however, vulnerable to faults of processor and software. To overcome the disadvantages, the concept of segment and partition in a channel has been developed. Each segment in a channel is divided from sensor to reactor trip and engineered safety features, which is based on the functional diversity of input signals against the various plant transient phenomena. Each partition allocates the function module to an independent processing module in order to process and isolate the faults of each module of a segment. A communication system based on the deterministic protocol with the predictable and hard real-time characteristics has been developed in order to link the various modules within a segment. The self-diagnostics including on-line test and periodic test procedures are developed in order to increase the safety, reliability and availability of DPPS. The developed DPPS uses the off-the-shelf DSP(digital signal processor) and adopts VME bus architecture, which have sufficient operation experience in the industry. The verification and validation and quality assurance of software has been developed and the architecture and protocol of deterministic communication system has been researched.

1. 서론

원자력 플랜트의 계측제어 계통은 현재 급속히 디지털화가 진행되고 있다. 기존의 아날로그 계통의 단점인 드리프트, 열화(aging), 유지보수의 어려움, 인적 오류의 발생 가능성 등과 같은 단점을 디지털 계통은 신호의 디지털 처리와 유연한 설계로 극복할 수 있기 때문이다.[1][2] 특히 자가 진단이나 온라인 시험 등과 같은 기능을 이용하여 계통의 안전성, 신뢰성과 가용성을 높이는 것이 가능하기 때문에 디지털 계통은 기존의 아날로그 계통보다 안정적인 운전을 가능하게 한다.[3] 현재 디지털 제어계통의 설계는 완성 단계에 있으나 플랜트 보호계통은 디지털 계통의 단점인 소프트웨어 오류 발생 가능성을 정량적으로 평가하기 어렵고 하드웨어적으로는 내부 구조가 복잡한 마이크로프로세서의 도입으로 규제 요건을 만족시키기가 어려워 현재 부분적인 연구가 진행되고 있다.

본 논문에서는 위와 같은 디지털 계통의 단점을 세그먼트와 분할 개념을 도입함으로써 기능적인 다양성을 확보하여 정성적으로 극복할 수 있는 디지털 플랜트 보호계통의 구조를 연구하였다. 보호계통의 한 채널의 기능을 입력 신호에 대한 기능적인 다양성을 확보하는 세그먼트로 분산시키고 또한 세그먼트 내의 기능을 각각의 기능 모듈별로 할당하여 하나의 프

로세서 이상 상태 발생시에도 적절한 조치를 수행할 수 있는 기능적 다양성을 확보하였다.

세그먼트내의 기능에 대한 연구를 수행하였고 특히 디지털 계통의 장점인 자가 진단 및 온라인 시험 기법에 대한 연구를 수행하였다. 그리고 세그먼트내 각 프로세서간의 연결은 결정론적인(deterministic) 통신망으로 연결하여 그 메시지의 오류 발생에 대한 대비 기능을 개발하여 기존의 아날로그 계통의 복잡한 구조를 상대적으로 단순화시켰다.

현재 연구가 진행중인 단계로써 디지털 계통의 인허가에 직접적으로 관련되는 소프트웨어 개발에 관련된 품질 보증과 확인 및 검증에 관련된 내용과 통신망의 세부 프로토콜 및 사양은 계속 개발되고 있는 단계이다. 그리고 디지털 보호계통의 구체적인 안전성, 신뢰성, 가용성과 성능은 추후 진행되는 원형(prototype) 개발을 통해 정성적인 그리고 정량적인 해석이 수행될 예정이다.

2. 디지털 플랜트 보호계통의 구조

전형적인 보호계통의 구조는 네 개의 채널로 다중화된 구조를 가지며 각각은 독립성을 유지하도록 설계된다.[4] 각 채널의 기능은 크게 입력 자료를 취득, 분석하는 자료취득 기능, 각 채널별로 입력신호의 상태에 따른 트립(trip)이나 예비트립(pretrip)을 판단하는 트립 비교 기능, 각 채널로부터 취합된 트립과 예비트립 신호에 대한 일치성을 판단하는 동시논리 판단 기능 그리고 원자로정지 신호와 공학적안전설비 개시 신호를 생산하는 출력 기능으로 크게 나눌 수 있다.

기존의 아날로그 계통과는 달리 디지털 계통은 소프트웨어의 오류나 프로세서의 내부적인 오류에 대한 단점을 가지고 있다. 이러한 단점을 극복하기 위하여 하나의 채널은 신호 흐름을 기준으로 수평적으로는 입력 신호를 분산시키는 세그먼트 개념을 도입하고 수직적으로 각 기능별로 할당된 분할 개념을 이용한다. 그림 1에 본 연구에서 개발된 디지털 보호계통의 개략적인 구조가 나타나 있다. 보호계통의 각 채널의 기능에 따라 각각의 프로세서를 할당하였으며 모든 채널은 서로 동일한 구조를 가지므로 대표적인 A, B 채널만 표시하였다.

수평적으로 분산된 세그먼트 개념은 플랜트 입력 신호를 플랜트 과도 현상에 따라 다중처리할 수 있도록, 하나의 과도 현상에 직접적으로 연관되는 두 변수를 두 세그먼트 각각으로 분산 입력하여 하나의 세그먼트에서 디지털 특성에 따른 알 수 없는 이상 상태 발생시에도 보호계통 전체 입장에서 트립 신호를 발생시키는 데 문제가 발생하지 않도록 하는 개념이다. 이는 디지털 계통이 복잡한 프로세서를 기반으로 소프트웨어 구동 방식을 이용하므로 소프트웨어 오류나 프로세서 내부의 오류에 대한 기본적인 방어 기법으로 사용된다. 이미 다중화되어 있는 채널 개념에 덧붙여 한 채널 내에서 입력 변수의 기능적 다양화 방어 개념을 도입하는 것이다. 구체적인 안전해석과 각 세그먼트의 고장모드-효과분석이 수행되어야

만 정확한 세그먼트 분산이 이루어지나 현재 대표적인 세그먼트로 분산되는 신호의 예는 증기발생기 각각에 대한 압력, 수위에 대한 두 신호를 다른 세그먼트로 분산시키는 것을 고려하고 있다. 서로 다른 세그먼트로 분산시키는 것이 불가능한 가압기 압력과 같은 신호는 두 세그먼트 모두의 입력 신호로 선정하여 하나의 세그먼트 오류에 대한 대비를 할 수 있다. 현재 개념상 설정된 플랜트 과도 현상에 대한 입력 신호의 세그먼트 분산은 표 1에 나타나 있다. 그리고 하나의 세그먼트는 그림에 나타난 바와 같이 하나의 채널과 마찬가지로 채널 내부의 모든 기능을 수행하는 각 기능 모듈들로 다른 세그먼트와 독립적으로 구성된다.

수직적으로 기능이 할당되는 분할 개념은 각 세그먼트 내에서 자료취득 기능, 트립 비교 기능, 동시 논리 판단 기능, 원자로 정지 및 공학적안전설비 개시 신호 발생 기능을 각각의 기능 모듈로 할당하여 상호 독립적으로 기능을 수행할 수 있도록 하는 개념이다. 이 역시도 세그먼트 개념과 유사하게 각 기능별 처리 과정에서 알 수 없는 오류에 대한 방어 대책으로 하나의 기능 모듈에서 정상 신호가 발생하지 않는 경우에 그 다음 기능에 할당된 모듈에서 이전 기능 모듈의 오류에 대한 처리 기능을 수행하도록 설계하는 개념이다. 결론적으로 세그먼트와 분할 개념으로 디지털 계통이 가지는 단점 중의 하나인 구동 소프트웨어와 기능 모듈 내부의 알 수 없는 오류에 대한 극복 방안으로 한 채널 내에서 기능적으로 다양화된 방어 대책을 확보하였다.

디지털 보호계통의 각 세부기능은 아날로그 보호계통과 유사하게 수행한다. 자료취득 기능 모듈은 각종 센서들의 아날로그 신호를 디지털 신호로 변환하는 A/D 변환 기능을 수행하여 디지털 기능 수행이 가능하도록 하는 기능이다. 디지털 입력 신호를 처리하므로 다양한 부가 기능을 고려할 수 있으나 보호계통의 특성상 입력 신호에 대한 검증과 같은 신호의 왜곡을 불러 올 수 있는 다양한 기능을 수행하지는 않고 센서의 특성 변화를 살피기 위한 제한적인 한계치 검사만을 수행한다. 트립 비교 기능 모듈은 공정 변수와 기설정된 설정치(setpoint)를 비교하여 트립 상태를 결정한다. 그리고 설정치 유형에 따른 설정치 변경 알고리듬과 운전원 우회에 관한 처리 기능을 가진다. 동시논리 판단 기능 모듈은 각 채널별 세그먼트 별 트립 상태를 입력으로 2/4 혹은 2/3 동시 논리 판단을 수행하며 유지보수를 위한 채널 우회 기능을 가진다. 원자로 정지 및 공학적안전설비 개시 신호 발생 기능 모듈은 동시논리 판단 기능에서 확인된 트립 신호를 각 구동단으로 전송한다. 그리고 디지털 계통의 장점인 각 기능 별 온라인 시험을 위한 기능이 추가되어 있으며 각 세부 기능은 다음 장에서 상세히 설명한다.

그리고 각 세그먼트 내부의 신호 연계를 위해서 디지털 계통의 장점인 공통의 신호 선로를 사용하는 통신망을 사용한다. 각 세그먼트 별로 독립된 통신망을 구축하며 한 채널내의 통신망은 독립성 요건을 저해하지 않으므로 서로 연계된다. 통신망은 보호계통의 내부 구조를 간단하게 하고 복잡한 신호 연결선을 사용하지 않고 다량의 디지털 신호를 각 기능 모듈

로의 전송을 가능하게 한다. 하지만 공통의 신호 선로를 이용하고 여러 개의 모듈 신호가 전송되므로 정해진 시간 내에 기능 수행에 요구되는 신호의 정확한 전송과 전송 오류에 대한 처리 기능을 가지는 결정론적 구조를 가져야 하며 또한 보호 계통 내부의 신호 전송을 위한 충분한 용량을 가져야 한다. 현재 통신망 부분은 구체적인 프로토콜과 하드웨어적인 사양에 대한 연구가 진행중이다.

디지털 보호계통의 신뢰성 확보 측면과 기존의 아날로그 보호계통의 높은 가격 문제를 극복하기 위해 보호계통만을 위한 특정한 구조가 아니라 현재 일반 산업계와 특수 응용 분야에서 많이 이용되어 신뢰성이 확보되어 있는 VME 버스와 빠른 연산 수행 및 적절한 신뢰성을 확보하고 있는 DSP를 프로세서로 이용하는 디지털 보호계통의 개발 연구를 수행하고 있다.

3. 디지털 보호계통 기능

전체적인 보호계통의 기능은 기존의 아날로그 계통과 유사하며 디지털 계통 설계에 따른 차이는 다음과 같다. 전체적인 보호계통의 기능 블록도는 그림 2와 같다.

3.1 트립 비교 기능 모듈

각 세그먼트 당 한 개의 트립 비교 프로세서가 있으며 각각은 다수의 공정 변수에 대한 트립 비교 기능을 수행한다. 각 트립 비교 프로세서는 예비트립과 트립 신호들을 결정하는 기능을 실행한다. 예비트립은 공정 변수가 원자로정지 혹은 공학적안전설비 제한치에 근접함을 나타내고 트립은 감시되는 공정변수가 한계치를 넘는 것을 나타낸다. 개략적인 기능 블록도는 그림 3에 나타나 있다.

발전소 과도 상태에 대한 사고완화 측면에서 분석된 공정변수를 각 트립 비교 프로세서에 할당한다. 하나의 사고완화를 위한 공정 변수가 여러 개 존재하면 각 공정 변수를 각각 다른 트립 비교 프로세서에 할당하는 방식으로 분할되어 있다. 이는 하나의 프로세서 이상 상태 시에도 모든 공정 변수에 대한 트립 기능을 상실하지 않고 각 과도현상에 대한 다중화된 트립 기능을 제공하기 위함이다.

트립과 예비트립의 상태들은 트립 비교 출력과 인가된 운전 우회(operating bypass)에 의해 결정된다. 운전우회가 존재하면 트립과 예비트립은 발생하지 않는다. 트립 비교 알고리듬은 예비트립과 트립 출력상태를 결정한다. 측정된 디지틀 공정값과 설정치 알고리듬(setpoint algorithm)으로부터의 기설정값(예비트립 과 트립)을 비교하여 결정된다.

운전우회(operating bypass)는 플랜트의 정상적인 시동(startup) 및 정지(shutdown)와 저출력 시험(low power testing)이 가능하도록 제공된다. 운전우회 알고리듬은 운전우회 허용

을 자동으로 제어하기 위하여 외부 생성 디지틀 데이터와 디지틀 입력값을 이용한다. 외부적으로 생성된 수동운전우회 요구는 운전우회를 제어하는 운전우회 알고리듬에서 허용신호(permissive)와 논리적으로 “AND" 된다.

3.2 동시논리 판단 기능 모듈

각 세그먼트마다 한 개의 동시논리 판단 프로세서가 있다. 각 동시논리 판단 프로세서는 각각 할당된 트립을 위해 동시논리 판단을 제공한다. 프로세서에 할당되는 트립은, 트립 비교 기능 모듈과 동일하게, 최적의 동시논리를 위하여 과도 응답에 대한 완화 측면에서 분석된 입력 변수를 할당한다. 각 동시논리 판단 프로세서는 생성되는 트립 상태들을 다른 채널에서 입력을 받는다. 그리고 운전원 모듈에서 채널 유지 보수를 위한 채널 우회 기능을 제공하며 하나의 채널 우회 시에는 동시에 다른 채널이 우회되지 않는 연동 기능을 설정한다.

3.3 자가 진단 및 온라인 시험 기능

디지털 계통은 계통 내부의 이상 상태에 대한 온라인 자가 진단 기능을 소프트웨어적으로 구현할 수 있다.[5][6] 각 기능을 수행하는 프로세서마다 자체적인 시험을 수행하여 이상 상태를 탐지하며 이상 상태 발생시에 운전원 모듈에 이상 상태를 표시하여 운전원의 인지 하에 유지 보수 작업이 가능하도록 설계한다. 그리고 자가 진단 및 온라인 시험 기능을 시험이 불가능한 센서 후단부터 A/D 변환이전까지의 이상 상태와 원자로 정지 및 공학적안전설비 개시 신호 발생 후단부터 구동기까지의 건전성은 기존의 아날로그 보호계통이 수행하는 것과 같은 주기적인 시험 기능도 가진다. 이때 내부의 RAM, ROM, 프로세서 상태에 대한 종합 진단도 같이 수행한다. 설계된 자가 진단 및 온라인 시험 기능은 다음과 같은 항목에 대한 내용을 포함한다.

- 감시타이머(watch-dog timer) : 감시타이머를 이용한 프로세서 잠김(lock) 상태를 확인한다. 감시 타이머는 정해진 주기마다 프로세서를 리셋 함으로써 논리 연산의 오류와 처리능력은 시험하기 어려우나 잠김 상태에 대한 건전성은 확인 가능하다.
- 논리 연산 검사 : 프로세서의 논리 연산의 오류를 검사하기 위해 미리 정해진 수식을 연산하여 그 결과와 미리 정해진 결과를 비교하여 논리 연산의 오류를 확인한다.
- 메모리 검사 : 각 프로세서의 RAM과 ROM의 건전성을 검사한다. ROM의 건전성은 초기 기동 시에 검사합(checksum)을 미리 정해진 값과 비교하여 ROM의 건전성을 시험하고 주기적인 검사 과정 동안에도 같은 검사를 수행하여 ROM의 건전성을 확인한다. RAM의 건전성 확인은 메모리 값이 고정된 영역과 가변적인 영역을 나누어 시험하며 고정된 영역은 ROM과 유사한 방법으로 건전성을 확인한다. 값이 가변적인 영역은 ROM과 같은 검사합을 계산한 후에 가변적인 영역의 모든 비트를 역으로 변환시켜(inverse) 검사합을 구하고 두

검사합의 차이가 적절한 지를 계산하여 가변적인 영역의 건전성을 확인한다.

- 전송메시지에 검사 : 통신망을 통해 전송되는 메시지의 건전성을 확인하기 위하여 자체 메시지 내용을 그대로 전송하고 두 번째로 RAM 검사와 유사하게 전송 메시지의 모든 비트를 역으로 변환하여 CRC 검사를 수행한다. 각 CRC 검사 결과에 따라 전송 메시지의 건전성을 확인한다. 이 부분은 세부적인 내용이나 오류 발생시에 재전송 요구와 같은 세부 구조는 현재 개발 중이다.
- 주기적인 시험 : 주기적인 시험은 기존의 아날로그 계통과 유사한 방법으로 수행되며 디지털 검사에 따른 시험 기능은 자가 진단 및 온라인 시험과 유사하게 수행한다.

3.4 그 외 기능

그 외 기능은 기존의 아날로그 계통과 동일하므로 따로 기술하지 않고 다만 자료 취득 기능 모듈에서 입력 신호의 건전성을 시험하기 위해 온라인으로 연속적인 한계치 검사를 수행한다.

4. 소프트웨어 설계

소프트웨어 설계는 구조적 기법에 의한 모듈 설계 방식을 채택하고 각 기능 모듈별 소프트웨어를 생산한다.[7] 현재 디지털 보호계통의 쟁점이 되고 있는 사항으로 구체적인 소프트웨어 품질보증과 확인 및 검증을 위한 절차와 요건을 개발 중에 있으며 이는 실제 보호계통 원형(prototyping) 제작을 통해 구체적으로 입증할 예정이다. 특히 소프트웨어 명세 확인 및 검증을 위한 Z, Colored Petri-Net, Statechart 등과 같은 formal 기법에 대한 검토가 수행중이다.

실제적으로 소프트웨어 코딩은 하드웨어와의 일치성 유지 그리고 투명한 확인 및 검증을 위해 각 프로세서의 하드웨어에 적절한 어셈블 언어를 사용하고 있고 그 외 상용 실시간 운영체제와 컴파일러 등에 대한 사용은 배제하고 있다. 실제 코딩은 3장에서 설명된 보호계통 기능별 모듈을 설계하고 모듈간의 연계를 설계하고 전체를 통합하는 방식으로 진행한다.

5. 결론

본 논문은 디지털 보호계통의 개발을 위해 디지털화에 따른 특징과 장점을 논의하였고 예상되는 문제점을 해결하는 하드웨어적인 구조와 기능을 개발하였다. 개발된 구조는 디지털의 단점으로 나타나는 내부 오류들에 대한 극복 방안으로 수평적인 세그먼트와 수직적인 기능 분할을 이용하였다. 세그먼트와 분할 구조는 내부적인 오류에 대하여 기능적인 다양성을

이용하는 개념이다. 그리고 계속되는 연구를 통해 실제 디지털 플랜트 보호계통에 대한 구체적인 세부 사양 및 소프트웨어를 개발한다. 특히 소프트웨어 개발과 확인 및 검증에 대한 추가적인 연구가 요구되며 개발된 디지털 보호계통의 개념은 앞으로 구체적인 원형 제작을 통해 세부 사양의 구현 및 소프트웨어 코딩이 이루어진다. 원형 제작이 완성되면 실제 보호계통이 가져야 하는 성능에 대한 확인 작업을 수행하고 그리고 보호계통의 기능 수행 시에 필수적으로 요구되는 신뢰성 분석 및 안전성에 대한 확인 및 검증 작업이 수행될 예정이다.

Acknowledgement

본 연구는 과학기술부의 원자력연구개발사업 일환으로 수행되었다.

[참고문헌]

1. 구인수 외, 일체형원자로 MMIS설계기술개발, KAERI/RR-1901/98, 1999.
2. 구인수 외, SMART 계측제어시스템의 신기술 적용방법, KAERI/AR-496/98, 1998.
3. N. Storey, Safety-Critical Computer System, Addison-Wesley, 1996.
4. 울진원자력발전소 3,4호기 최종안전성분석보고서, 한국전력공사.
5. M. Lubaszewski and B. Courtois, A Reliable Fail-Safe System, IEEE trans. on Computer, Vol. 47, No. 2, pp236-241, Feb., 1998.
6. H. Y. Chung and Z. Bien, Real-Time Diagnosis of Incipient Multiple Faults with Application for Kori Nuclear Power Plant, J. of the Korean Nuclear Society, Vol. 27, No. 5, pp670-683, Oct., 1995.
7. E. Yourdon, Modern Structured Analysis, E-Hahn Publishing Co, 1994.

표 1. 세그먼트 별 공정 입력 변수

트립변수 / 과도현상	SG1 low P	SG2 low P	CONT high P	SG1 low L	SG2 low L	SG1 △P	SG2 △P	SG1 high L	SG2 high L	PZR low P	PZR high P	LOG PWR	VOPT
급수온도 감소	1*	2*											
급수유량 증가								1	2				
주증기유량증가	1	2											
증기관 파단	1	2											
복수기진공상실								1	2				
급수 상실				1	2								
냉각재유량상실						1	2						
부적절보론희석												2	1
제어봉 인출												2	1
냉각재 고압력											1,2		
냉각재상실사고			1,2							1,2			

주)

1) 1* - **세그먼트** 1

2) 2* - **세그먼트** 2

3) CPC(CORE PROTECTION CALCULATOR)**에서 입력되는 신호는 두 세그먼트로 모두 전송된다**.

4) **약어 설명**

- L(Level)
- P(Pressure)
- PWR(Power)
- VOPT(Variable Overpower Trip)
- H-H (High-High)
- CONT(Containment)
- SG(Steam Generator)
- PZR(Pressurizer)

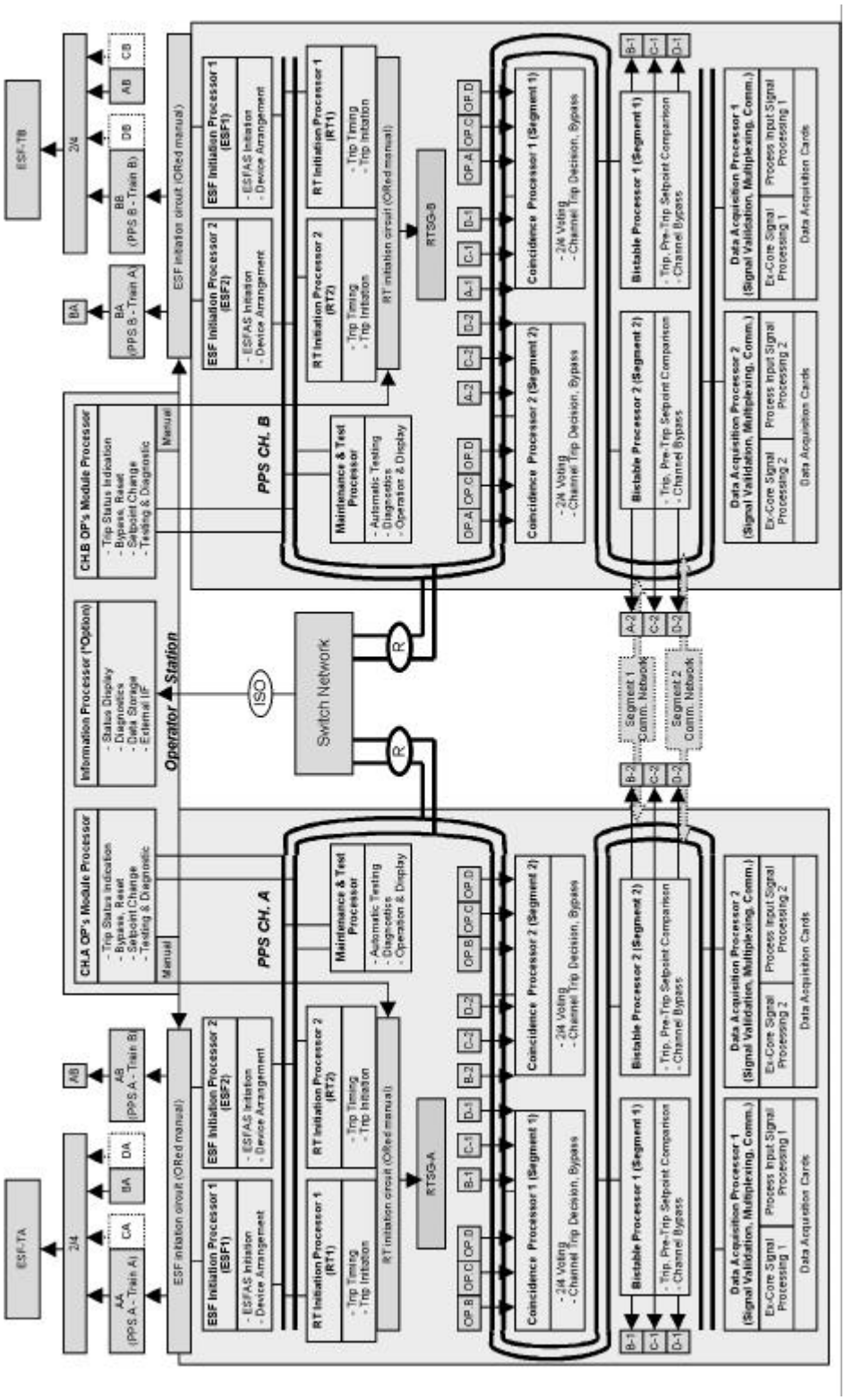

그림 1 디지털 플랜트 보호계통의 구조도

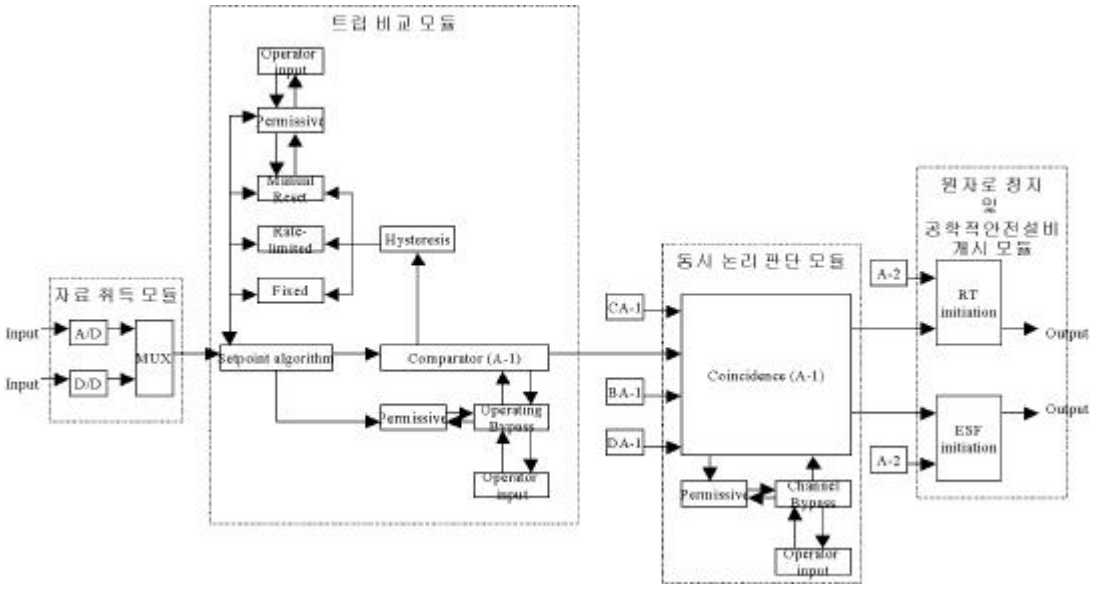

그림 2 디지털 플랜트 보호계통의 기능블록도

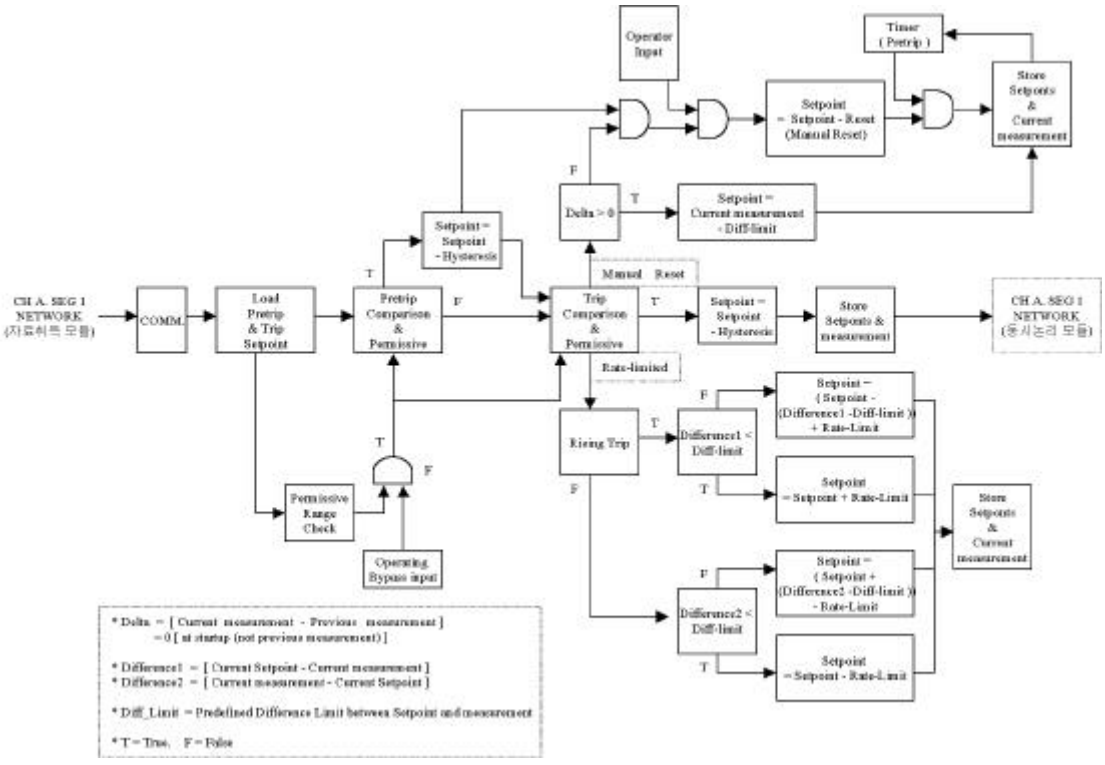

그림 3 트립 비교 기능블록도