

## 원자력 발전소 분산 제어 시스템을 위한 고신뢰 통신망의 설계

이 성 우\*, 임 한 석\*

(한국전력공사 전력연구원, "건국대학교 전기공학과")

### Design of a Reliable Network for DCS in Nuclear Power Plant

Sung Woo Lee\* and Han Suck Im\*

\*Korea Electric Power Research Institute and "Dept. of Electrical Engineering Kon-Kuk Univ.

**Abstract** - In this paper, a highly reliable communication network for DCS in nuclear power plant is designed. The structure and characteristics of DCS in nuclear power plant is briefly explained. The features needed for a communication network for DCS in nuclear power plant is described. According to the above features, the layer structure of the communication network is determined and each layer is designed in detail.

#### 1. 서 론

분산 제어 시스템은 제어 기능이 한 곳에 집중되므로써 발생하는 여러 문제를 해결하기 위해 나온 시스템으로서 이름 그대로 제어 기능이 여러 개의 작은 제어 장치에 분산된다. 즉 분산 제어 시스템의 특징은 제어 기능은 분산시키고 반대로 정보 처리 및 운전 기능은 집중화시켜 신뢰성을 향상시키고 데이터의 관리를 원활하게 하는 데에 있다. 분산 제어 시스템에서 분산되어 있는 각 제어 장치는 통신망을 통해 연결되어 정보를 교환하게 된다. 이는 다시 말하면 통신망은 분산 제어 시스템에서 중요한 하나의 부분이라고 할 수 있으며 통신망의 성능, 신뢰성, 안정성 등에 따라 분산 제어 시스템의 성능, 신뢰성, 안전성이 좌우된다는 것을 의미한다. 각 제어 장치들의 안전성과 신뢰성이 아무리 높더라도 이들을 연결하는 통신망이 불안정하면 결국 그 분산 제어 시스템은 불안정하고 신뢰할 수 없는 시스템이 되는 것이다. 그러므로 통신망의 안전성 및 신뢰성은 분산 제어 시스템에서 매우 중요한 문제가 되며 만약 분산 제어 시스템의 적용 대상이 원자력 발전소라면 그 중요성은 더욱 부각된다.

원자력 발전소에 적용되는 분산 제어 시스템의 통신망을 설계하는 경우에는 원자력 발전소용 통신망을 설계할 때 고려해야 하는 사항들을 충분히 반영해야 한다. 그러한 사항들도 다음과 같은 것들이 있다[1].

- 통신망이 상태기반(state-based) 시스템인가 사건기반(event-based) 시스템인가를 파악하고 알맞은 형태의 통신망 규약을 선택한다.
  - 그 시스템을 구성하는 노드들간의 데이터 송수신과 관련된 사항이 알려져 있어야 한다.
  - 통신 시스템은 결정적(deterministic)이어야 한다.
  - 통신망의 규약, 그 통신망에 사용되는 실제 매체와 관련된 요구 사항을 파악하고 이에 맞게 설계해야 한다.
- 본 논문에서는 위와 같은 사항을 충분히 고려하여 원자력 발전소에 사용되는 분산 제어 시스템을 위한 고신뢰 통신망을 설계한다. 여기에 분산 제어 시스템에서 각 제어 장치를 연결하는 통신망이 가져야 하는 요건들을 살펴본다. 그리고 이러한 요건을 충족시킬 수 있도록 통신망의 계층적 구조를 정한다. 그리고

각 계층을 상세히 설계한다. 통신망 하드웨어에 대한 설계도 언급한다.

본 논문은 다음과 같이 구성된다. 2장에서는 원자력 발전소 분산 제어 시스템의 일반적인 구조를 설명하고 특성을 제시한 후 이 분산 제어 시스템을 위한 통신망이 가져야 할 요건을 제시한다. 3장에서는 통신망의 계층 구조 및 계층별 설계에 대해 기술한다. 4장에서 본 연구의 결론과 앞으로의 과제를 제시한다.

#### 2. 통신망의 요건

이 절에서는 원자력 발전소 분산 제어 시스템의 전체적 구조 및 특성에 대해 살펴보고 분산 제어 시스템을 위한 통신망의 요건을 제시한다. 앞서서도 언급한 바와 같이 분산 제어 시스템에서는 분산되어 있는 각 부분을 연결하는 통신망이 매우 중요한 부분으로 부각된다. 일반적으로 분산 제어 시스템은 다계층 구조를 가지는데 가장 중요한 통신망은 분산된 제어 장치를 연결하는 통신망이다. 이러한 통신망은 중위 계층 통신망이라고 볼 수 있다.

중위계층 통신망은 여러 개의 단위 분산 제어 시스템을 연결하는데 사용된다고 할 수 있다. 이렇게 연결된 시스템들은 하나의 제어와 감시 등의 기능을 수행하는 그룹을 형성하게 된다. 이러한 경우 중위계층 통신망에서 가장 중요한 것은 긴급한 상황에서 발생하는 데이터를 최대한 빨리 전송하는 것이다. 또한 중위계층 통신망은 주기적으로 반복되는 데이터를 잘 처리해야 한다. 마지막으로 중위 계층 통신망은 사용가능성이 있는 고급 서비스를 제공할 필요가 있다. 즉 본 논문에서 제시하는 분산 제어 시스템의 중위계층 통신망이 가져야 하는 구체적인 특성은 다음과 같이 정리된다.

- 긴급한 데이터의 실시간 전송
  - 주기적 데이터의 효율적 처리
  - 다양한 고급 서비스의 제공
- 원자력 발전소에 사용되는 분산 제어 시스템의 중위계층 통신망은 위의 요건을 만족시킬 수 있어야 한다.

#### 3. 통신망의 설계

이 절에서는 앞에서 살펴본 요건들을 바탕으로 원자력 발전소 분산 제어 시스템을 위한 통신망을 설계한다. 이하에서는 이 통신망을 PICNET-NP (Plant I&C Network - Nuclear Power Plant)라고 칭한다.

##### 3.1 통신망 계층 구조

일반적으로 통신망은 3계층 또는 7계층 구조를 가진다. 물리 계층, 데이터 링크 계층, 그리고 응용 계층만으로 이루어지는 것이 3계층 구조이고 세션 계층, 데이터 링크 계층, 네트워크 계층, 트랜스포트 계층, 물리 계층, 프리젠테이션 계층, 응용

계층으로 이루어지는 것이 7계층 구조이다. 3계층 구조는 계층 구조가 단순하므로 실시간성을 확보하는 측면에서 유리하다. 그리고 최상위의 응용 계층에서 고급의 서비스를 제공할 수 있다. 7계층 구조의 경우 최대의 장점은 송수신 신뢰성을 높일 수 있다는 것이지만 계층 구조가 복잡하므로 시간이 오래 걸려서 실시간성을 확보하기 어려우며 그렇다고 제공하는 서비스가 3계층 구조에 비해 크게 다양한 것도 아니다. 따라서 7계층 구조는 분산 제어 시스템을 위한 통신망으로는 부적합하다. 이 논문에서는 원자력 발전소 분산 제어 시스템의 중위계층 통신망의 계층 구조를 3계층으로 정한다. 그리고 이 3계층 외에 통신망 관리(network management) 부분이 포함된다. 이 부분은 통신망의 신뢰성 및 성능을 높이고 오류를 관리하기 위해 꼭 필요한 부분이 된다.

이상의 내용을 종합하여 본 연구에서 원전 DCS 중위계층을 위한 통신망은 그림 1과 같은 구조로 설계된다.

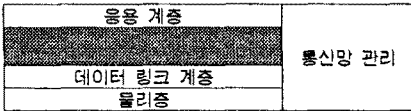


그림 1. 원전 DCS 중위계층 통신망의 구조

### 3.2 물리 계층

PICNET-NP의 물리 계층은 IEEE 802.3 CSMA/CD 방식(2)을 채택한다. 그러나 뒤에서 설명하겠지만 데이터 링크 계층의 MAC 부계층은 IEEE 802.4 토큰 버스 방식(3)을 채택한다. 따라서, MAC 부계층과 물리 계층 사이의 서비스가 IEEE 802.4와 IEEE 802.3 방식을 각각 만족시켜야 한다. 따라서, PICNET-NP의 물리적 신호 방식은 IEEE 802.3의 방식을 그대로 따른다. 한편, IEEE 802.4 방식의 MAC 부계층-물리 계층 접속 서비스 규격을 만족해야 하므로, PICNET-NP의 PLS 부계층은 IEEE 802.3 표준의 PLS 부계층 접속 서비스를 IEEE 802.4 표준의 MAC 부계층-물리 계층 접속 서비스로 변환하는 기능을 담당한다. 즉, PICNET-NP의 물리 계층은 IEEE 802.3 표준의 물리 계층에 IEEE 802.3 표준의 PLS 부계층 접속 서비스 변환 기능을 추가한 것이다. 그림 2는 PICNET-NP의 물리 계층과 인접 계층과의 서비스 관계를 나타낸 것이다.

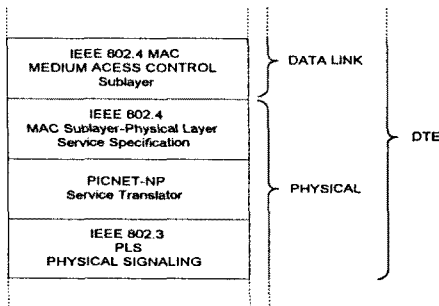


그림 2. 물리 계층과 인접 계층과의 서비스 관계

PICNET-NP의 물리 계층은 여러 가지 특성을 가진다. 그것들을 간략히 나열하면 다음과 같다.

- 1) 생산성, 시험성, 안전성 및 신뢰성 : 고신뢰성과 실시간성을 충족시키는 통신 방식으로서 토큰 전달 방식이 사용되었다.
- 2) 다양한 제품군의 지원 : 한편, 보편적인 기술로 널리 사용되고 있는 IEEE 802.3 기술 혹은 Ethernet 기술은 그 시장의 확대를 말미암아 다양하고 폭넓은 제품의 선택이 가능하다.
- 3) 기존의 통신망 활용 가능 : 기존에 IEEE 802.3용 통신망이 설치되어 있다면 이들을 그대로 이용할 수 있다.
- 4) 적절한 통신 속도 : 그간의 연구 결과에 의해 적당하다고

판단되는 속도를 만족하도록 하였다.

5) 산업용으로도 적합한 전기적 규격 : 또한, IEEE 802.3 방식의 물리 계층은 산업용으로 사용되고 있는 각종 통신망 시스템의 각종 전기적 규격에 미달되지 않는다.

### 3.3 데이터 링크 계층

데이터 링크 계층은 매체 접속 제어 부계층(media access control sublayer)과 링크 제어 부계층(link control sublayer)을 사용하고 있다. 매체 접속 제어 부계층은 IEEE 802.4 토큰 버스 규약(3) 표준을 따르도록 설계되었고 링크 제어 부계층은 IEEE 802.2 논리 링크 제어(logical link control) 규약(4) 표준에 자체적으로 주기 서비스를 할 수 있도록 하는 부분을 추가하여 설계되었다.

매체 접속 제어 부계층에서 토큰 버스 규약을 채택한 것은 이벤트성의 트래픽 전송을 효율적으로 하기 위한 것이다. IEEE 802.4 토큰버스 프로토콜은 불규칙적으로 발생하는 메시지의 양이 적은 평소에는 스테이션들 사이에 토큰을 전달하기 위한 오버헤드가 있기 때문에 프리런 타입 스케줄링 기법보다는 효율이 다소 떨어지지만 일시에 많은 양의 트래픽이 발생한 경우에는 비교적 신속히 처리할 수 있다.

링크 제어 부계층에서는 IEEE 802.2 논리적 링크 제어 규약을 기본으로하여 약간의 기능을 추가하였다. LLC 부계층은 논리적 링크를 구성하고 데이터를 전송하는 역할을 한다. 이 논문에서는 IEEE 802.2 논리 링크 제어 규약에 정의된 nonacknowledged connectionless 방식인 유형 3을 동시에 지원하는 클래스(class) 3를 구현한다.

긴급 서비스와 고급 서비스에서는 통상의 IEEE 802.2 논리 링크 제어 규약과 같이 동작한다. 그러나 주기 서비스를 할 경우에는 주기적으로 깨어나는 프로세스가 존재하여 지정된 시간이 되면 비어 있는 데이터를 유형 3의 응답 서비스를 이용하여 전송하도록 한다. 이 논문에서는 주기 서비스를 위한 이러한 부분이 IEEE 802.2 논리 링크 제어 규약 위에 약간 추가되어 링크 제어 부계층이 구성된다.

### 3.4 응용 계층

응용계층은 통신망의 기능을 이용하려는 응용 프로그램을 구현할 때 제반 기능을 제공한다. 일종의 통신 서비스 라이브러리라 가 된다. 그림 3에 응용 계층의 서비스를 보았다. 응용 계층의 구조는 다음과 같이 세 부분으로 이루어짐을 알 수 있다.

먼저 긴급 서비스 부분이다. 사건에 의해 촉발되는 응용 프로세스는 긴급하고 중요한 데이터의 송수신에 사용된다.

다음으로 주기 서비스 부분이다. 주기적인 응용 프로세스는 일정한 시간 간격으로 데이터의 송수신을 하는데 사용된다. 이러한 프로세스는 주기성을 만족하는 것이 중요하다.

마지막으로 고급 서비스 부분이다. 통신망을 초기화 하거나 환경 설정을 할 경우 혹은 대량의 데이터 등을 송수신 하는 경우에는 시간적인 제약이 중요하지 않게 된다. 이러한 경우에는 서비스의 사용의 편리함 등이 요구되는데 이러한 기능을 제공하는 서비스가 응용 계층의 고급 서비스이다.

위와 같이 세 부분으로 나눈 근거는 안전성과 신뢰성을 높이기 위함이다. 물론 구조를 보다 간단하게 할 수 있는 방법도 있다. 예를 들면 첫째로 하나의 서비스를 사용하여 필요에 따라 긴급 서비스로, 주기 서비스로 또는 고급 서비스로 동작하도록 구현할 수도 있고, 둘째로 모든 응용 계층의 서비스를 긴급 서비스로 혹은 주기서비스가 되도록 구현할 수도 있다. 그러나 첫 번째의 경우에는 하나의 서비스가 다양한 기능을 수행하기 때문에 사용자(응용 계층을 사용하는 프로그래머)의 입장에서는 편리할 수도 있으나 프로그램 중에 실수를 할 가능성이 커진다. 또한 하나의 함수 내에서 많은 판단 부분이 들어가기 때문에 속도의 저하를 유발한다. 이러한 것들은 안전성과 신뢰성을 떨어뜨리게 된다. 두 번째 경우는 응용계층의 모든 서비스를 긴급 서비스로 혹은 주기 서비스로 사용하도록 제공하게 되는 경우인데 이 경우에는 사용자도 편리할 수 있고 응용 계층을 구현하는 프로그래머도 작업의 부담이 많이 줄어든다. 그리고 응용

계층이 단순해 짐으로써 오류 가능성이 줄어든다. 이런 장점이 있는 반면 이러한 형태는 우선 순위라는 것을 무시한 형태가 되어 시스템의 위기 상황(Emergency)에 대한 효율적인 대책을 마련하기가 곤란해진다. 즉, 시스템 전체적으로 안전성과 신뢰성의 저하를 가져오게 된다. 따라서 본 논문에서는 위에서 설명한 바와 같이 세 부분으로 나누어 응용 계층을 구현한다.

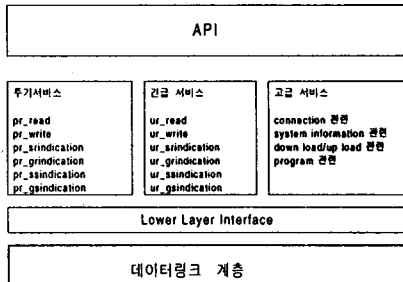


그림 3. 응용 계층의 서비스

### 3.5 통신망 관리

PICNET-NP에서의 통신망 관리의 PICNET-NP의 하드웨어 및 소프트웨어와 관련된 환경 설정과 유지 보수를 위한 역할을 수행한다. PICNET-NP에서의 통신망 관리 계층은 통신망 관리 기능을 수행하는 서비스와 이 서비스를 위해서 정의된 자료 구조(data structure)로 이루어진다. 또 다른 통신망 계층과의 접속이나 원자력 발전소 시스템의 특성을 고려한 안정성 및 신뢰성 확보 대책 등도 함께 고려된다.

PICNET-NP의 통신망 관리 기능을 종류별로 나누어 보면 구성 관리 기능과 오류 관리 기능 그리고 원격 관리 기능이 있다. 안정성 및 신뢰성 확보 대책과 관련하여 PICNET-NP의 통신망 관리에서는 오류 관리 기능의 일환으로 이중화 관리 기능을 제공한다.

구성 관리의 역할은 다음과 같다. 먼저 통신망의 초기화와 관련된 설정을 해준다. 그리고 통신과 관련된 중요한 파라미터들을 관리하고 이들의 값을 읽거나 원하는 값으로 설정한다. 두 번째로 오류 관리의 역할은 다음과 같다. 오류 발생을 감지하고 이것을 기록하고 보고한다. 이러한 오류 발생과 함께 이중화 관리 기능을 수행한다. 마지막으로 원격 관리의 역할은 다음과 같다. 통신망 상의 다른 스테이션의 중요한 구성 정보를 읽어 오거나, 구성 관련 자료를 다운로드하기 위한 명령을 내리는 등의 역할을 원격 관리가 수행한다. 그리고 긴급한 상황에 대처하기 위한 방안으로 다른 스테이션의 통신 기능을 중단하라는 명령을 내리기도 한다.

### 3.6 하드웨어

PICNET-NP의 하드웨어는 크게 호스트 프로세서부와 통신망 접속부로 구분될 수 있다. 여기서 호스트 프로세서부는 사용자 프로그램이 실행되거나 혹은 사용자 프로그램이 실행될 수

있는 환경을 제공해 주는 부분이며 통신망 접속부를 제어하게 된다. 통신망 접속부는 VME 버스를 통해서 전송될 데이터 혹은 수신된 데이터를 호스트 프로세서부와 주고 받게 된다. 통신망 접속부에 대한 설명은 물리 계층에서 이미 하였으므로 여기에서는 호스트 프로세서부에 대해서 다룬다. 그림 4는 PICNET-NP 하드웨어의 블록도이다. VME 버스 인터페이스를 지원한다.

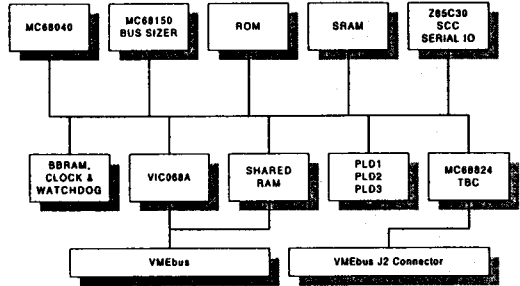


그림 4. PICNET-NP 하드웨어의 호스트 프로세서부

## 4. 결 론

본 논문에서는 원자력 발전소 분산 제어 시스템에 적용할 통신망을 설계하였다. 원자력 발전소 분산 제어 시스템을 위한 통신망이 갖추어야 할 요건을 제시하고 이에 따라 통신망의 계층 구조 및 각 계층을 설계하였다.

원자력 발전소라는 응용 분야는 안전성 및 신뢰성이 아주 크게 요구되는 분야이다. 따라서 원자력 발전소 분산 제어 시스템을 위한 통신망 개발시에 중요한 것은 검증 및 확인(verification & validation) 과정을 거치는 것이라고 할 수 있다. 앞으로 원자력 발전소 분산 제어 시스템을 위한 통신망의 검증 및 확인 과정에 대해 연구하는 것이 반드시 필요하다고 할 수 있다.

### (참 고 문 헌)

- [1] G. G. Preckshot, Data Communications, NUREG/CR-60S2, Lawrence Livermore National Lab., 1993.
- [2] ANSI/IEEE 802.3 CSMA/CD Access Method, 1987.
- [3] ANSI/IEEE 802.4, Token-Passing Bus Access Method, 1987.
- [4] ISO/IEC 8802-2, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 2: Logical Link Control, 1994.