분산제어시스템 이중화 구성방안에 대한 검토

김응석, 오영일
전력연구원 발전연구실

An Implementation of Redundancy Design for Distributed Control System

Eung-Seok Kim and Young-il Oh
Korea Electric Power Research Institute

Abstract - 본 논문은 국산 개발 분산제어시스템의 신뢰성을 향상시키기 위하여 Power Supply System, Control Processor, Communication System에 대한 이중화 구조를 분석하고 외국 시스템과의 비교를 통해 국산 시스템의 미비점을 파악하고 이를 개선하기 위한 이중화 구조 설계 방안을 제시하고자 한다.

1. 서 론

1970년대 초반 반도체 및 Computer 분야의 발달로 인해 등장한 마이크로프로세서 기술은 산업공정제어분야에 큰 영향을 미쳐 오늘날의 디지탈 분산제어시스템(Distributed Control System, DCS)을 등장케 했다. 분산제어시스템은 발전소와 같이 대규모이고 프로세스가 복잡한 구조를 갖는 산업공정의 제어시스템으로 널리 보급되어 사용되어지고 있는데 공정제어에 있어 가장 중요한 점은 시스템의 신뢰성이다. 시스템의 신뢰도는 고장 발생의 빈도 및 정도에 의해 결정되는데 최근에는 신뢰도의 향상을 위해 Fault Tolerant 방법이 많이 사용되고 있으며 실제 적용에 있어 대부분 하드웨어 Redundancy에 의해 이루어져 있다.

본 논문에서는 Y화력의 보일러 프로세스에 적용 예정인 국산 개발 분산제어시스템의 이중화 구조에 대하여 분석하고 현재 화력발전소에 설치 운용중인 외국 제품의 이중화 구조와 비교 검토하고자 한다. 각기 독자적인 시스템 구성 형태를 갖고 있으므로 절대적인 비교 평가는 어렵지만 이중화 구성 설계시 가장 중요시되는 전원공급 설비와 주제어모듈, 통신계통에 대해 하드웨어 측면에서 검토하고자 하며 향후 국산 개발 분산제어시스템의 Fault Tolerant 시스템 설계시 고려해야 할 사항들에 대하여 기술하고자 한다.

2. 본 론

2.1 System Architecture

분산제어시스템의 기본 Architecture는 전원공급설비, 제어 Station, Operator Station, I/O Station, Communication System으로 구성되며 전체 시스템의 신뢰성 확보를 위해서는 전원, 제어, 통신 설비는 반드시 이중화 구조로 설계되어야 만 한다. 그림 1은 국산 개발 분산제어시스템인 MASTER P-3000 시스템을 이용한 보일러 프로세스용 제어시스템의 설계도면으로서 운전원의 조작 및 감시를 위한 Workstation Display Center(WDC), 각종 엔지니어링 데이터 및 제어로직의 설계 및 수정을 위한 Engineering Workstation System(EWS), 제어부인 MPU(Main Process Unit)와 입출력부인 I/O 및 입출력 처리부인 Interface Shelf가 내장되어 제어 및 연산 기능을 수행하는 Remote Control Station(RCS), 시스템 내의 모든 데이터에 대한 관리 및 처리를 행하는 Database Processing Center(DPC), 이들 시스템을 연결하는 통신 네트워크로 구성된다.

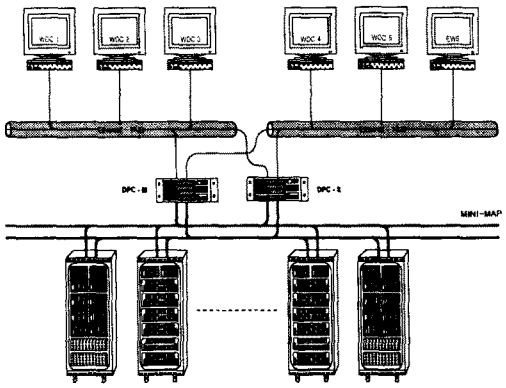

그림 1. Master P-3000 System Architecture

2.2 Power Supply System

분산제어시스템의 전원공급 설비는 신뢰도 측면에서 매우 중요한 의미를 갖는데 각 제작사의 제어시스템에 따라 표준화된 전원장치가 공급되며, 시스템에 따라 사용전압의 크기 및 종류가 다르고 전원공급 방식이 상이하기 때문에 제어시스템 선정시 전원공급설비의 구비기능 및 신뢰도에 대한 검토가 이루어져야 하며 전원상실에 의한 제어시스템의 Trouble를 방지하기 위하여 전원공급 장치의 입출력에 대한 이중화 설계가 요구된다.

가장 일반적인 이중화 구성 방안은 그림2의 (b) 또는 (c)와 같이 전원장치를 이중화하고 입력 전원은 서로 다른 source의 전원을 공급받아 입력전원 또는 전원장치 중의 한 대가 고장이 나도 제어시스템에 별다른 영향이 없이 전원공급을 계속 유지하도록 하는 것이다.

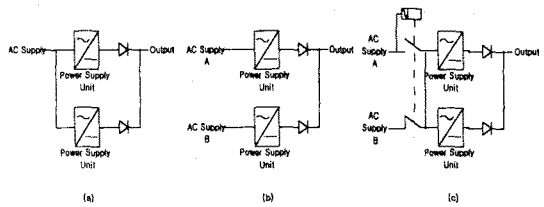

그림 2. Typical Power Supply Arrangement

2.2.1 INFI-90 System(Bailey)

INFI-90의 Modula Power System의 전체적인 구성도는 그림 3과 같으며 AC/DC 압을 입력 받아 380 VDC까지 승압한 후 DC/DC Converter에 의해 System(+5, ±15, 25.5VDC) 및 Field(25.5, 48, 125VDC)용 전원을 공급한다. Redundancy 구조는 단순한 이중화의 개념이 아니고 N, N+1, N+x, 2N의 구조로 구성이 가능하여 사용자가 선택하도록 설계되어 있다. 이 전원공급설비의 특징으로는 다양한 입력 전

압의 사용 가능, Load Sharing, Power Monitoring, On-line 교체, Input Power Factor Correction 등이 있다.

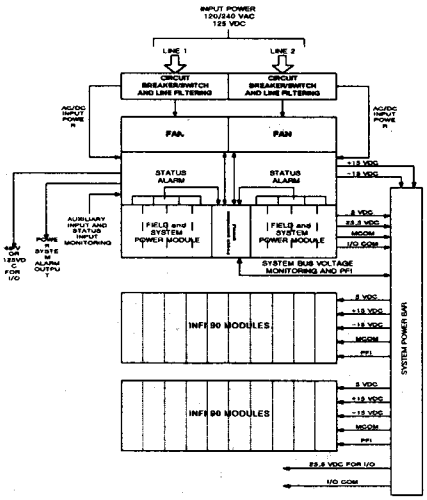

그림 3. Modular Power System II Architecture

2.2.2 MASTER P-3000 System(LG)

Master P-3000의 전원공급설비는 AC 220V를 입력받아 +5V DC, ±12V DC, +15V DC, +24V DC를 출력으로 사용하며 기본 구성도는 그림 4와 같다. 구성기기로는 PDU(Power Distribution Unit), SPS(System Power Supply), APS(Analog Power Supply), DPS(Digital Power Supply)가 있으며 전원 공급은 Shelf 단위로 구분하여 공급하도록 되어있다.

이중화 구조를 살펴보면 우선 전원모듈의 입력 전압이 그림 2의 (a)와 같이 단일 source에서 공급되도록 되어 있어 입력전압 상실시 전원 모듈의 이중화가 무의미하며 전원 모듈의 이중화도 I/O Shelf에만 적용되었고 주제어 기능을 하는 MPU(Main Processor Unit)에는 적용하지 않아 공급 전압의 상실시 정상 동작중인 MPU의 절체(Master-->Slave)를 가져오도록 설계되어 있다. I/O Shelf용 전원 모듈 이중화 방식은 Master 전원 모듈에서 100% 부하를 담당하다가 고장시 대기 중이던 Slave 전원 모듈이 부하를 담당하는 Back-up 방식을 적용하였는데 이 방식을 적용하는 경우에는 전원모듈 개별로 출력상태 및 정상동작 여부를 감시하여 이상시 경보를 발생시키는 전원감시 기능 및 On-line 교체가 가능해야만 시스템의 신뢰도를 더욱 향상 시킬 수 있다. 그림 5는 Y화력에 설치 예정인 Master P-3000 시스템의 신뢰성을 보다 확보하기 위한 전원공급설비의 이중화 구성 설계 개략도이다.

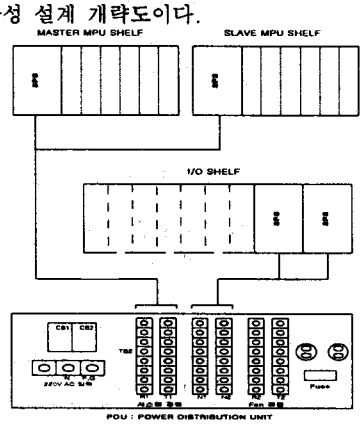

그림 4. MASTER P-3000의 기본 전원 계통도

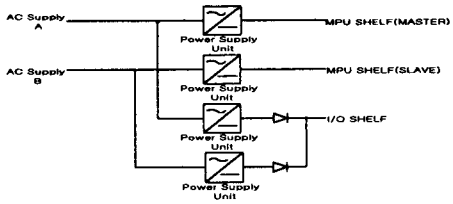

그림 5. 신뢰성 확보를 위한 이중화 구성

2.3 Control Processor

공정제어에 있어 분산제어 시스템의 신뢰성을 위해서는 제어 기능을 담당하는 제어 모듈의 안정된 동작이 최우선이므로 필수적으로 Redundancy System을 구성해야만 한다. Redundancy 구조는 통상 Backup Processor의 동작 형태에 따라 Hot-Standby와 Cold-Standby 구조로 분류할 수 있는데 Hot-Standby 구조는 동작중인 Active Processor에서 Fault 발생시 Backup Processor가 Processing의 중단 없이 수행해 나가는 방식이고 Cold-Standby 구조는 Active Processor가 동작중일 때는 Backup Processor가 대기하고 있다가 Fault 발생시 동작하는 방식이다. 그러므로 Cold-Standby 구조는 주기적으로 Active Processor의 Data와 Status를 Update 해야 한다. 종래의 분산제어 시스템은 Cold-Standby 구조를 사용하였으며 Fault 신호 감지 및 Processor의 절체를 위해 별도의 Fault Detection 모듈이 필요하였는데 이 모듈의 고장시 Backup Processor의 작동 자체가 불가능하다는 단점이 있었다. 최근에는 별도의 Fault Detection 모듈이 없이 그림 6과 같이 똑같은 두 개의 Processor로 구성되며 Hot-Standby 동작을 하는 Fault Tolerant Processor가 보편화 되고 있다.

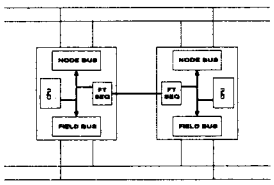

그림 6. Fault Tolerant Processor

2.3.1 Multi-Function Processor(Bailey)

INFI-90 설비의 제어모듈인 MFP(Multi Function Processor)의 이중화 구조는 1 Mbaud Serial Link (그림 7의 P3 Link)에 의해 구성되며 이 선로는 RS422 방식에 의해 데이터를 통신하고 DMA(Direct Memory Access) 기능이 있어 Backup MFP가 Hot-Standby 동작을 하면서 Active MFP의 이상시 10[msec]이내에 절체되어 Active MFP의 모든 기능을 대체할 수 있다.

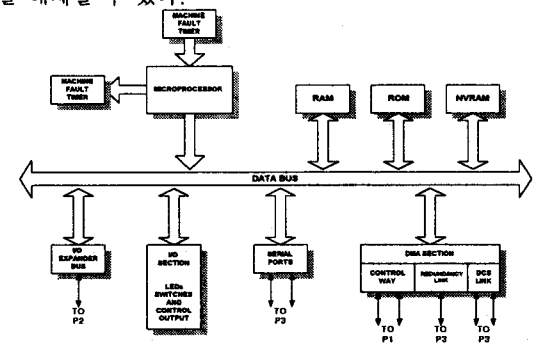

그림 7. MFP Hardware Block Diagram

2.3.2 Main Processor Unit(LG)

Master P-3000 System의 주제어 Unit인 MPU(Main Processor Unit) Shelf는 1 대 1의 Cold-Standby 이중화 방식을 채용하였으며 그림 8은 MPU Shelf의 이중화 구성을 나타낸다. Redundant MPU Shelf로의 절체는 DLU (Data Link Unit) 모듈에 의해 이루어 지는데 이 모듈은 Master/Slave MPU Shelf에 각각 내장되어 VME Bus를 통하여 상대의 MPU Shelf를 감시하고 Function Block에 관련된 출력 및 파라메타 등을 갱신하여 등치화 하는 기능을 수행한다. Infi-90의 MFP의 이중화 구조와 비교해 보면 다음과 같은 단점이 있다. 첫째, 앞에서 언급했듯이 DLU 모듈의 고장시 Backup MPU Shelf의 동작 자체가 불가능하고 둘째, Shelf 단위로 이중화 구성을 하였기 때문에 불필요한 절체 요인이 많다.

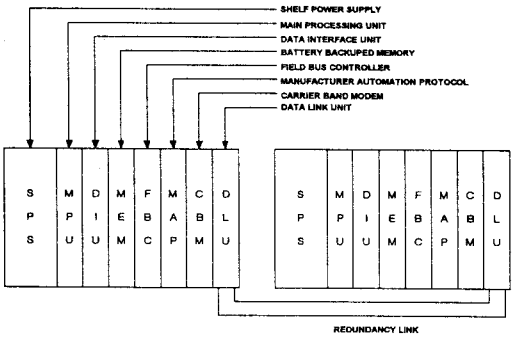

그림 8. MPU Shelf의 이중화 구성

2.4 Communication Network

분산제어시스템은 Plant의 여러지역에 분산되어 있는 제어 개소를 각각 제어하면서도 전체의 Plant를 동일한 Real Time System으로 통합제어 하고자 하므로 통신 기능에 있어 여러 Level의 통신 Network을 상호 유기적으로 Error없이 고속으로 Data를 전송하는 것이 중요하다. 분산제어시스템의 통신 네트워크를 분류해 보면 통상 Data Highway라 하는 Node Bus와 I/O System과의 통신을 위한 Field Bus 그리고 Operator Station간의 통신을 위한 Network으로 구분할 수 있다. 통신 네트워크의 이중화 구성 설계에 있어 신뢰성을 향상시키기 위해서는 다음과 같은 사항이 고려되어야 한다. 첫째, 네트워크 이중화시 Dual Port Processor로 구성해야만 한다.(그림 6 참조) 둘째, 통신 Port가 Optical Isolation 되어 있어 일부 통신 매체에 고장이 발생되더라도 네트워크 전체의 통신에는 문제가 없는 구조이어야 한다.

2.4.1 이중화 구조 분석(LG-Net)

Master P-3000 시스템의 Data Highway는 LG-NET이라 명칭하며 구성도에서 보는바와 같이 시스템의 통신 방식으로는 Dual Network이 사용되며 공장 자동화용 프로토콜인 Mini-Map방식을 적용하여 리얼타임 처리가 가능하며, RCS에서 발생되는 현장의 데이터를 상태변화시만 보고되는 Exception Report방식으로 대규모의 시스템에서 통신의 혼잡을 피하고 대용량 고속 데이터 수집이 가능하도록 되어있다. 그리고 DPC와 상위 시스템(WDC, EWS)와의 접속에는 범용의 TCP/IP 프로토콜이 사용된 Ethernet을 사용하였다. 전체 통신 시스템의 이중화 구조는 그림 9와 같으며 이중화 기능 점검 결과 다음과 같은 단점이 있다. 첫째, 각각의 MPU Shelf에 내장된 통신 모듈인 MAP(Manufacturing Automation Protocol)과 Mini-Map 간의 통신이 MPU 별로 분산되어 있지 않아 동작중인 MAP 모듈중 하나라도 고장이 발생하면 전체 Mini-Map Line의 절체가 발생한다. 둘째, 대기중인 통신 Line의 고장시 경보 발생 기능이 없어 네트워크의고장을 사전에 방지하기 어렵다.

Field Bus는 MPU Shelf내의 FBC(Field Bus Controller)와 I/O Shelf내의 DCU(Data Control Unit)간의 Bus로서 RS-485방식에 의한 통신을 하느데 이중화 구조를 보면 FBC 모듈에 Dual Port 설계를 적용하지 않아 DCU 모듈의 절체시 MPU Shelf 및 Mini-Map의 절체를 발생시킨다.

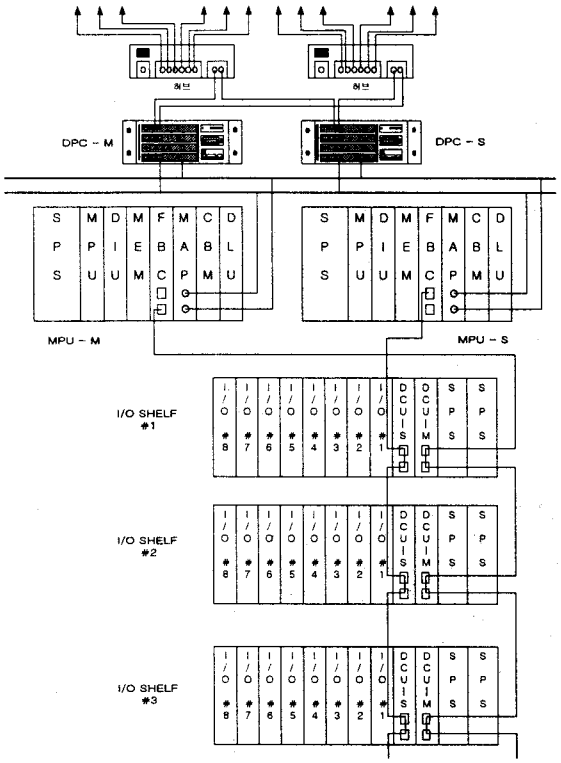

그림 9. Master P-3000 Network 이중화 구성도

3. 결 론

본 고에서는 국산 개발 분산제어시스템의 이중화 구조 및 현재 운용중인 외국제품과 비교 분석하였으며 지금까지 살펴 본 바와 같이 분산제어시스템의 신뢰성을 향상시키기 위해서는 이중화 구조의 설계가 매우 중요하다. 특히, 전원공급시스템의 경우 어떠한 경우에도 정원장치의 고장에 의한 제어시스템의 Down이 발생하지 않도록 X-Y Matrix방식의 설계가 요구되며 통신 시스템은 모든 Port가 고장에 대한 파급 현상을 줄이도록 각각 Isolation되어야만 한다.

[참 고 문 헌]

[1] 남희우, "Fault Tolerant Open Architecture System", 월간 제어계측, 10월호,18~25p, 1997

[2] 김은기외2, "울산화력 및 삼랑진 양수 발전소 데이터로깅 시스템 개선연구", 최종보고서, 1997

[3] 변증남외7, "분산제어 시스템의 고장 대처 기능 및 제어언어의 구현", 최종보고서, 1993

[4] 신영달, "Boiler Backup Control을 위한 Multiprocessor 방식에서의 신뢰도 개선에 관한 연구, 과학기술원 석사학위논문, 1987

[5] Bailey사, "Infi-90 System Training Manual"

[6] LG사, "Master P-3000 System Manual"