제어시스템의 보팅에 관한 현장 적용 사례 연구

신윤오, 김종안 (전력연구원)

A study of Fault Tolerance Voting Systems that have been applied to plants

Shin Yoon-Oh, Kim Jong-An (KEPRI)

요약문

산업이 발전해 가며 공장 자동화를 하는 회사는 나날이 늘어가고 있으며 현재 산업 전반에 걸쳐 자동화 시스템을 채택하지 않는 곳을 찾아보기 어렵고 이 시스템의 시험 및 운영자 교육용으로 시뮬레이터에 대한 관심은 높아 가고 있는 실정이다. 여기에서는 한국전력에서 사용하고 있는 터빈 제어 삼중화 시스템이 어떠한 보팅 기법들을 적용하여 설계되었으며 그 기능이 어떻게 구현되었는지를 실제 제품의 사례분석을 통해 검토해 보고자 한다. 검토 대상은 삼중화 제어기에 대해서만 시행할 예정이다. 이는 실제 현장이 경제성을 수반한 제어기의 신뢰, 이용, 안정, 수행, 지속, 시험, 확실성 등을 원하고 있으며 또한 시뮬레이터를 설계하는 사람들에게 삼중화 주제어기에 대한 비교(MARK-V, Triconex-TMR, GE-Fanuc, Woodward-Micronet) 소개함으로서 더욱더 현장과 가까운 시뮬레이터를 설계할 수 있도록 하기 위함이다.

1. 서 론

내고장성 시스템중에서 가장 많이 채택되고 적용되는 시스템은 TMR(Triple Modular Redundancy)과 대기-예비기법(Standby-Sparing)이라고 할 수 있다. 후자는 대기하는 방식에 따라 다소 다르기는 해도 재설정을 위한 적은 시간 동안 시스템을 중단해도 이상이 없는 대부분의 산업에 가장 경제적으로 적용할 수 있는 내고장성 시스템이다.

반면에 TMR 구조는 시스템의 일부 고장(single point failure)에 대해서 그 고장을 차폐하여 그것이 외부로 전달되지 않고 연속적으로 동작할 수 있는 시스템이다. 특히 다중화 시스템(NMR) 중에서 TMR은 3개의 홀수 다중화를 택함으로서 다중화 시스템에서 필수적인 다수결의 보팅(majority voting) 설계가 용이하게 되고 확보되는 신뢰도에 비해 가장 경제적이고 현실적인 시스템 구성이라 할 수 있다. 본 논문에서는 TMR 시스템의 구성에 있어서 중요한 보팅 설계에 대해 사례를 들어 검토해 보기로 한다.

2. 본 론

가. 입력 보터 (Input Voter)의 구성

- TMR I/O : 각 제어기가 동일한 입력에 대해서 독립적인 센서 혹은 외부입력을 받는 시스템으로서 제어기뿐만 아니라 외부의 센서, 입력배선까지도 3중화하게 된다. 이러한 구조의 입력은 터빈 제어의 과속도 검출용 MPU(Main Process

Unit)나 밸브의 위치를 검출하는 LVDT(Linear Variable Differential Transformer) 등의 적용에서 볼 수가 있다.

- Parallel I/O : 외부에서의 센서 입력은 하나이지만 그것이 주제어기로 전달되는 것이 병렬로 된 입력구조를 말하며 각 제어기는 일반적으로 각각 독립된 입출력 모듈을 가지게 되며 한 입력모듈의 고장이 다른 건전한 입력모듈의 입력을 방해하지 않도록 전기적, 기계적으로 분리하는 것이 필요하다. 이 방식의 입출력은 시스템 구성에 있어 Critical 하지 않는 많은 입력의 처리에 유용하며 감시전용일 경우 입력모듈 자체를 병렬로 하여 H/W를 감소시킬 수 있다.

어떤 방법을 사용하든지 TMR의 각 주제어기들은 입력정보를 갖게 되며 그것으로 제어·연산을 수행하게 된다. 아날로그 입력의 경우 센서의 오차, 입력모듈의 A/D 에러 등으로 인하여 각 제어기는 동일한 출력을 낼 수가 없으며 따라서 출력의 보팅을 어렵게 할 수 있다. 또 적분기를 가진 제어기로 구성된 TMR의 경우, 최종 출력에서 선택되어 제어에 기여하지 않는 제어기는 포화되어 고장 발생시 이 제어기가 사용될 때 시스템의 Bump가 발생될 수 있다.

이러한 이유로 대부분의 TMR 구조의 제어시스템은 입력 보터를 사용하게 된다. 그러나 입력보터의 사용은 시스템의 H/W를 증가시키고 따라서 전체적인 시스템 신뢰도 저하를 가져올 수 있다.

따라서 대부분의 시스템들은 위에서 언급한 입력보터의 필요성과 입력상태의 진단을 위하여 SIFT (Software Implemented Fault Tolerance) 개념의 입력 보터를 사용한다. 각 제어기간의 통신버스를 통하여 다른 제어기에서의 입력 데이터를 공유함으로서 각 제어기는 독립적으로 입력보팅을 수행하게 되며 그 결과로 제어연산을 수행한다. 또 데이터의 공유로 다른 데이터와의 비교, 다수결의 보팅을 통하여 입력의 고장상태를 검출할 수 있게 되는 것이다.

이러한 방식의 입력보터 구성을 위해서는 보팅의 동기화를 위하여 고속의 전용 통신망이 사용되는데 Mark V에서의 DENet(Data Exchange Network), TRICON의 TRIbus가 그 사례이다.

나. 주제어기와 통신 버스

TMR에서 3중화된 제어기는 일반적으로 아래와 같은 데이터/통신 버스를 가지고 있다.

I/O 버스는 입출력 모듈과 주제어기 사이의 데이터 전송을 위한 버스로서 입출력 모듈의 접속방식이나 주제어기의 구성에 따라 크게 2가지로 구분된다.

하나는 입출력 모듈 자체가 프로세서를 보유하고 있는 독립 모듈로 동작하고 주제어기와의 사이에는 통신을 통하여 입출력 데이터가 전달되는 분산 I/O 방식이다. Mark V의 I/O Net, GE-Fanuc Critical Control System에서의 I/O Bus 등이 여기에 속한다.

다른 방식은 TRICON 시스템이나 MicroNet/TMR 시스템처럼 VMEbus 구조를 채택하여 주제어기와 입출력 모듈을 연결하는 방식이다. 일반적으로 I/O 버스는 전술한 2가지 방식을 같이 사용하는 경우도 있는데 Non-Critical 감시전용 I/O에는 통신방식을, Critical 제어 전용 I/O는 버스방식을 사용하는 것이다. 통신방식은 I/O 모듈을 Local에 둘 수 있으므로 배선길이를 줄일 수 있고, 독자적이고 지능적인 I/O 모듈 자체의 진단기능은 강화되나 입출력의 속도는 상대적으로 낮다.

버스방식은 TRICON 시스템처럼 전용의 I/O

Bus를 사용하는 경우도 있고 GE-Fanuc의 PLC나 MicroNet 처럼 표준화된 VMEbus 혹은 PCI bus를 사용하는 경우도 있다.

Point-to-point 통신 버스는 TMR 구조에서 각 제어기간 데이터의 공유를 위해 사용되는 버스로서 입력과 출력의 보팅을 위하여 가장 중요한 버스이다. 보팅과 데이터의 공유는 TMR 시스템에서 동기화를 필요로 하므로 고속의 통신망을 이용하여 구현되게 된다. Mark V에서는 DENet(Data Exchange Network), TRICON에서는 TRIbus 등 2.5Mbaud 이상의 고속 통신망을 사용한다.

아래의 표1에 대표적인 TMR 시스템에서 적용되고 있는 버스의 종류와 사양을 정리하였다.

표 1. 버스의 종류와 사양

시스템 / 버 스	Mark V	GE-Fanuc	TRICON	MicroNet
I/O Bus	IONet	VMEbus Genius I/O Bus	IOBus 375Kbaud	VMEbus
Point-to-point 통신버스	DENet/ARCNet 2.5Mbaud	Genius bus	TRIbus 4Mbaud	RS232
상위 Link용 통신버스	-Stage Link -Modbus (19.2Kbaud)	-Modbus -Ethernet	COM bus 2Mbaud Ethernet	-PCMCIA 포트 -Ethernet/UDP -Serial port -Modbus

다. 출력보팅 시스템

H/W 여유설계 방식은 수동형, 능동형, 혼합형 시스템이 있으며 각각은 다수결의 보팅(majority voting), Watchdog Timer, Self-purging 기법 등이 있다. 그러나 실제의 내고장성 시스템들은 이러한 설계방식 중에서 한 개를 선택하여 구성되어 있는 것이 아니라 여러 개의 방식들을 결합하여 단순하면서도 신뢰성 높은 시스템을 구현하고 있다. 여기에서는 실제 시스템들이 구체적으로 어떤 보팅 시스템들을 채택하고 있으며 그 특징들이 무엇인가를 검토해 보기로 한다.

1) Mark V의 출력 Voter

Mark V에서의 출력 보터는 기본적으로 디지털 출력에만 적용하며 아날로그 출력에 대해서는 보터를 거치지 않고 3-Coil Servo Actuator로의 직접 출력인 Flux Summer 방식을 택하고 있다.

출력보터의 기능은 TCRA라고 하는 릴레이 구동보드에서 수행되고 있는데 여기에는 4개의 입력이 인가되어 보팅된 1개의 출력이 릴레이를 구동하는 구조로 되어 있다. 4개의 입력은 3중화된 각 제어기로부터 받은 개별적인 출력신호나 해당 제어기로부터의 1개의 기준 출력이다.

실제로 Mark V는 출력의 보팅에 있어 이 하드웨어적인 보터에만 의존하는 것은 아니고 각 3중화된 제어기 사이의 출력 데이터의 공유를 통해서 소프트웨어적인 보팅 절차를 거친 출력을 각 제어기가 내게 된다. 물론 제어기 자체의 보팅결과로부터 고장난 제어기를 인식하게 되고 그 결과는 기준 출력으로 반영되게 된다.

하드웨어 보터는 아날로그 회로로 구성되어 있는데 Self-purging 기법의 Threshold Gate 형식을 취하고 있다. 출력 보터의 구조가 다음의 그림 1에 나타나 있다

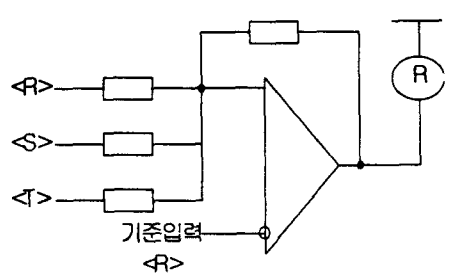

그림 1. Mark V의 출력 보터 구조

위의 그림에서 보는 것처럼 각 제어기로부터 출력은 가산기(Adder)의 형태로 보터회로에 입력되

는데 입력단의 저항치가 동일하면 동일한 가중치가 적용되는 것이다. 이 가중된 합(weighted sum)은 기준 신호와 비교되어 기준치보다 크면 출력 릴레이를 On시키게 된다. 기준신호는 현재 몇 개의 제어기가 건전한가에 의해 결정된다.

또 이러한 출력보터는 3중화되어 있어서 각 해당 제어기는 각각의 보터를 가지고 있으며 그 결과인 3개의 릴레이 출력은 최종적으로 Hard-wired Voter에 의해 1개의 접점 혹은 솔레노이드 출력을 내게 된다. 여기서 Hard-wired Voter란 접점의 상태를 배선을 이용하여 로직을 구성하는 것을 말하는데 2개 이상의 출력이 일치해야 최종적인 출력이 나가도록 직-병렬회로를 구성하는 것이다.

2) TRICON의 출력 모듈

TRICON TMR 시스템의 출력 보팅은 디지털 출력과 아날로그 출력 모듈에서 수행된다. TRICON의 출력 보팅은 전형적인 자기제거기법(Self-purging Redundancy)을 사용하는데 디지털 출력 모듈의 구조를 그림 2에 나타냈다.

독자적인 프로세서를 가진 출력 모듈은 3중화된 제어기로부터 각각 입력을 받아 보팅된 결과와 비교하여 일치하지 않을 때는 스스로가 제거되는 구조의 보팅구조를 채택하고 있다. 그림에서 보는 것처럼 1개의 출력모듈 내에서 Hard-wired 보팅까지 수행하므로 이 출력 모듈에 고장이 발생하면 제어기의 건전 여부에 관계없이 최종출력에 고장이 발생하므로 Hot 대기-예비기법(Standby Sparing)을 지원하는 동일한 모듈로 자동 교체되는 AutoSpare 기능을 갖고 있다.

TRICON 출력 모듈의 또 다른 특징은 Loopback 회로가 단순히 보팅을 위한 출력의 궤환을 거치지 않고 출력의 전압과 전류를 감시함으로써 부하의 개방, 단락, 전원상실 등 외부와의 인터페이스의 이상 유무까지도 검출하여 표시하는 기능을 가진다는 점이다.

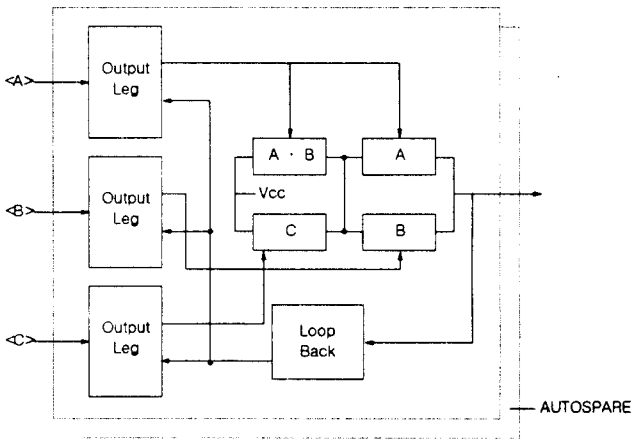

그림 2. TRICON 디지털 출력 모듈

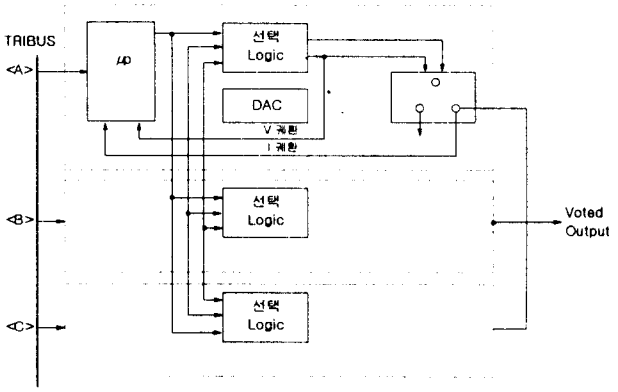

그림 3. TRICON의 아날로그 출력 모듈

아날로그 출력 모듈은 TRICON만이 갖는 특징 중의 하나이다. 이 아날로그 출력 모듈에서는 아날로그 보팅을 하게 되는데 그 구조를 그림 3에 나타냈다.

그림 3에서 보는 것처럼 한 개의 출력 모듈 내에 3개의 독립적인 Leg가 있으며 선택로직에 의해서 3개의 Leg중 한 개가 선택되어 최종출력으로 나가게 된다. 한 Leg에 고장이 발생하면 미리 정해진 순서에 의해 순차적으로 다른 Leg에서 출력을 내게 된다. 아날로그 출력 모듈도 각 Leg에

서 전압과 전류가 궤환되어 Leg 자체의 진단이 가능하다. 전류와 전압의 검출은 단락, 개방 등 외부회로의 상태를 정확하게 진단해 줄 수 있다.

3) MicroNet의 보터 구조

Woodward사의 MicroNet TMR 시스템은 GE사의 Mark V나 Triconex사의 TRICON 시스템과는 달리 Open Architecture의 VMEbus 구조를 갖고 있으며 후술할 몇 가지의 구조적인 특징을 가지고 있어 다른 두 시스템과는 차별성이 있다.

먼저 입력보터 부분을 살펴보기로 하자. 어떤 TMR 구조이든지 입력 보터가 H/W적으로 구성된 경우는 없고 모두가 SIFT 즉, 소프트웨어에 의한 내고장성 입력보터를 사용하고 있다. MicroNet의 입력보터는 SIFT의 개념은 동일하지만 보팅을 위한 데이터의 공유에 있어서 VMEbus를 버퍼링(Buffering)한 버스와 DPRAM(Dual Port RAM)을 이용한 버스의 이중교환 보터(Double Exchange Voter)의 사용이 특징이라 하겠다. 이렇게 함으로서 입력보팅의 신뢰성과 고속성이 보장될 수 있다. 입력보팅의 구조를 그림 4에 나타냈다.

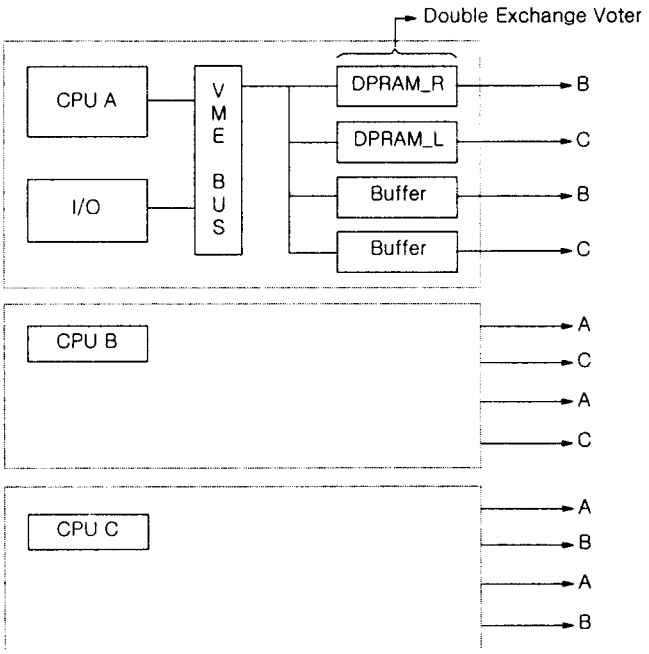

그림 4. MicroNet의 Input Voting 구조

아날로그 출력 모듈의 보팅 구조를 살펴보면 아날로그 출력은 각 제어기의 내부에서 소프트웨어적으로 보팅과정이 일어나고 그 결과가 출력 모듈을 통해서 외부의 Actuator 등으로 나가게 되며 아날로그 출력 모듈 그 자체의 기능은 전형적인 자기 제거 여유 설계(Self-purging Redundancy)를 적용하고 있다. 해당 제어기의 고장, 모듈의 고장, Watchdog Timer의 고장 등이 발생하면 모듈 자체를 제외시키고, 해당 채널이 고장나면 채널의 출력을 차단하는 구조로서 그 구성이 아래 그림5에 나타나 있다. 아래의 그림은 Dual Coil Servo Actuator에 적용한 아나로그 출력 모듈의 예로서 모듈 자신의 출력과 외부 조건의 검출을 위한 2중의 전압, 전류검출장치를 갖고 있는 전형적인 Flux-Summer의 형태이다.

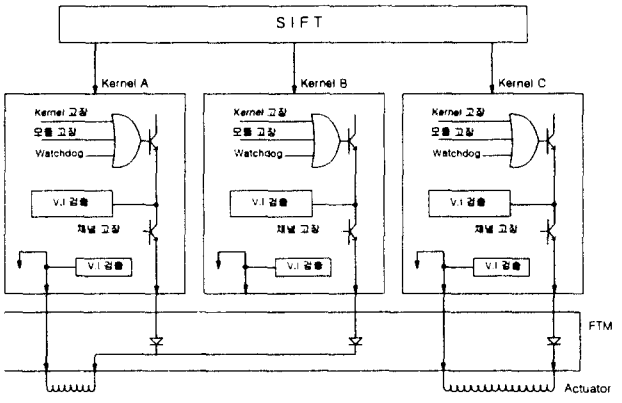

그림 5. 아날로그 출력 모듈의 구성

3. 결 론

대부분의 대용량 Power Plants에서 현재 사용하고 있는 Control System은 경제성에 우선을 두고, 중요 신호를 처리하는 것은 삼중화로 일반적인 신호처리는 이중화 방향으로 흘러가는 추세이며 어떤식으로 신호를 보팅하여 오신호에 의한 플랜트의 고장을 최소화시키냐는 문제는 크게 대두되고 있으며 새로운 제어시스템을 설계하고 현장에 적용시키기 위해서는 오랜 기간 정확한 시뮤레이션을 통하여 완벽한 시스템이 될 수 있게 설계함으로서 현장 운전원이 운전을 쉽게하고 정비를 쉽게 할 수 있도록 많은 노력을 기울려야 할 것이다. 본 논문에서 다룬 보팅 시스템의 실례는 매우 다양한 보팅 방법 중 빙산의 일각에 불과하며 보다 안정적이고 보다 신뢰성있는 제어 시스템을 설계하기 위해 다양한 보팅 방법에 대해 시뮤레이션 해 봄으로서 목적을 달성 할 수 있으리라 기대한다.

[참고문헌]

[1] Mark V Turbine Control User's Manual (GEH-5979B).

[2] Woodward, MicroNet Control System Product Specification (85583A).

[3] TRICONEX, TRICON Version 9 Systems

[4] Design and Analysis of Fault-Tolerance Digital System, Barry W. Johnson,

< 제출문 >

제목 : 제어시스템의 보팅에 관한 현장 적용 사례 연구

발표자명 : 신윤오

소속기관 : 한국전력 전력연구원 발전연구실 발전계전그룹

주소 : 대전광역시 유성구 문지동 103-16 (우편번호 : 305-380)

전화번호 : 042-865-5253

FAX : 042-865-5269

E-Mail : yoonoh@kepri.re.kr