FTCS(Fault Tolerant Control System)의 개발에 관한 연구

*문봉채, 조영조, 정현규, 김지홍, 변증남
한국과학기술원 전기및전자공학과

A Study on the Development of a Fault Tolerant Control System

*B.C.Moon, Y.J.Cho, H.K.Jung, J.H.Kim, Z.Bien
Electrical Engineering, KAIST

ABSTRACT

An FTCS is developed for the purpose of improving the reliability of a process control system. The proposed FTCS has capabilities of failure detection, back-up control, graphic display, and self-checking. Also the FTCS is combined with the process simulator to experiment in laboratory for the evaluation of performance of operation. The FTCS is applied to Thermal Power Plant.

I. 서 론

신뢰도를 향상시키는 문제는 항공 우주 분야, 원자력 발전 등과 같은 안전성을 요하는 분야에서나 공정 제어 분야와 같은 대규모 시스템에서 고장에 기인한 대형 사고 방지를 위해 연구가 활발히 진행되고 있으며, 오늘날에는 전자 기술의 발달로 제작 경비의 저렴화, 소자들의 신뢰도 향상이 이루어 짐으로써 각 분야에서 관심이 기울여 지고 있다.

본 연구를 통하여 제어 시스템의 신뢰도를 높이는 방안으로써 redundancy를 두고, 고장 진단을 수행하는 FTCS(Fault Tolerant Control System)를 제안하고, 이를 실제로 제작하여 실험을 수행하였다. 이 FTCS의 기능및 구성과 적용 실험을 위해 고려할 사항들에 대해서 설명하고자 한다.

신뢰도 향상을 피하는 방안으로써 (그림 1)과 같은 standby 구조를 생각할 수 있고, 대기 상태에 있는 모듈이 동작 준비가 항상 되어 있는 hot standby 구조와 필요할 경우에만 동작을 취하는 cold standby 구조로 나눌 수 있다.

본 FTCS는 제어 시스템 설계 관점이 아닌 기존의 제어 시스템의 보수 유지 단계에서 이를 추가함으로써 신뢰도를 개선시키도록 연구하였다. 또한 대규모 공정 제어 시스템을 대상으로 하였으며, 그 제어 시스템은 수십 내지 수백개의 제어 루프(loop)들이 결합되어 있고, FTCS의 고장 진단및 back-up 제어 단위는 이 제어 루프 1개에 대응한다. 수십 내지 수백개의 제어 루프들 중에서 동시에 고장이 발생하는 제어 루프는 1개 또는 기껏해야 2-3개 정도이므로 back-up 제어 가능 갯수를 4-8개 정도로 잡는 것이 경제적이다. 이렇게 하였을 경우 제어 루프당 cold-standby 구조를 띠게 된다.

II. FTCS의 구성및 기능

FTCS의 기능으로는 고장 진단, back-up 제어, 운전 메뉴 결정, 그래픽 디스플레이, 자체 고장 진단의 기능을 갖고, 실제 적용에 앞서 모의 운용 실험을 수행하기 위해 프로세스 시뮬레이터를 결합하였다. 또한 적용시 필요한 기능으로 제어기 파라미터 값 변경 기능, 제어 프로그램 변경 기능 등을 포함한다.

위의 기능을 수행하기 위해 FTCS는 man-machine interface 부분, 고장 진단 부분, 백업 제어 부분, 프로세스 시뮬레이터 부분의 4가지 부분으로 크게 구분한다.

man-machine interface 부분은 FTCS를 관리하는 기능과 그래픽 디스플레이 기능을 가진다. 1대의 단말기를 통하여 시스템 운전 메뉴를 결정 내리고, 1대의 모니터로 시스템의 상태및 제어 현황을 디스플레이 해준다.

고장 진단 부분은 기존의 제어기상의 고장 발생 유무를 탐지하는 기능을 갖는다. 각 back-up 단위별로 주어진 입력 측정치에 대하여 출력의 정격치를 계산한 후, 출력의 실제치와 비교하여 허용 범위를 넘어서는 가에 따라 고장 판단을 내리고 고장 내용을 공유 메모리를 통하여 각 부분에 전달한다.

back-up 제어 부분은 고장 발생 부위에 대하여 back-up 제어하는 기능을 갖는다. 4개의 D/A 변환 채널을 통하여 back-up 제어 신호가 출력되고, switching 부분에서 고장 발생 부위에 대한 출력 신호를 기존의 제어기에서 back-up 제어로 절환한다.

프로세스 시뮬레이터 부분은 모의 운용 실험을 위해 기존의 제어기와 플랜트를 모사(simulation)하는 기능을 갖는다. 또한 수동 조작 실험을 가능케 하기 위해 ON/OFF 스윗치와 배율기로 이루어진 operator station을 제작하여 결합하였다.

이상의 4개 부분이 결합하여 FTCS를 구성하고, 이는 실제로 1개의 HOST 컴퓨터와 3개의 SLAVE 프로세서로 구현하였고, 이들 상호간의 데이터및 정보 교환은 공유 메모리와 공유 버스(common bus)를 사용하여 이루어 진다.

HOST 컴퓨터와 SLAVE 프로세서 간에 교환되는 데이터로는 운용자가 키(key) 입력시킨 운전 메뉴, SLAVE 프로세서에 전송되어 실행될 object file등이 HOST로부터 SLAVE 프로세서로 전달되고, 그래픽 디스플레이를 위한 고장 정보및 제어 루프들의 입출력 데이터등이 SLAVE 프로세서에서 HOST로 전달된다. SLAVE 프로세서들 간에 교환되는 데이터로는 고장 정보, 입출력 데이터, 동기시키기 위한 각종 flag 등이 있다.

시스템 관리 기능으로 1대의 단말기를 통하여 시스템 운전 메뉴를 결정 내린다. 시스템 운전 메뉴는 다음과 같다.

i) 운전 시작 명령(S) : 데이터및 각종 flag들을 초기화시키고 자체 테스트를 수행한 후 각 프로세서 별로 작업을 수행하면서 동시에 시스템 자체 고장 진단을 실행한다.

ii) 운전 정지 명령(X) : 각 프로세서 별 작업및 시스템 자체 고장 진단을 중지시킨다.

iii) 자체 테스트 수행(T) : 시스템 하드웨어를 전반적으로 검사한다.

iv) 자체 테스트 정지(H) : 각 프로세서별 작업은 계속 수행하되 자체 고장 진단은 중지시킨다.

v) 자체 테스트 회복(R) : 자체 고장 진단이 정지된 곳으로부터 수행 계속한다.

vi) 모듈 테스트 모드(M) : 각 SLAVE 프로세서 모듈들을 개별적으로 테스트 하기 위해 debug monitor를 활용할 필요가 있을 때 쓰인다.

vii) 파일 전송 명령(L) : HOST 컴퓨터 내의 실행 object file을 SLAVE 프로세서로 전송한다.

viii) 제어기 파라미터 값 변경(P) : 제어기 파라미터 값을 변경시킬 때 쓰인다.

이 이외에도 다양한 그래픽 디스플레이 메뉴를 포함한다.

III. FTCS 적용 실험

공정 제어 시스템은 일반적으로 그 규모가 매우 크고, 안정성이 중요하다. 따라서 적용 실험도 FTCS 제작과정에서 수행하는 모의 운용 실험과 제작 후에 설치 운용 실험의 2단계로 구분하여 실험한다.

모의 운용 실험을 위해 프로세스 시뮬레이터 기능을 필요로 하고 이 기능은 설치 운용 실험시에도 테스트용으로 유용하게 쓰일 수 있다. 모의 운용 실험은 FTCS의 성능 평가 실험으로 고장을 임으로 발생시켜 이를 탐지해낸 후, back-up 제어를 수행하는 실험을 실시하여 이의 동특성 변화를 그래픽 디스플레이로 관찰하였다. (그림 2)는 FTCS의 성능 평가 실험의 한 예를 보인 것으로 고장 발생 시의 back-up 제어를 칼라 그래픽 디스플레이로 보여준다.

구현된 FTCS는 화력 발전소 보일러 제어기의 신뢰도 향상을 위해 실제로 설치 운용될 것이다. 따라서 설치 운용 실험을 수행하여야 하며, 이를 위해서는 다음 사항들을 고려하여야 한다.

첫째, 제어기 파라미터 값의 변경이 가능토록 하여야 한다. 발전소 설치 운용시에는 제어기 파라미터 값이 고정되어 있지 않고 가변성을 가지고 있음으로 이 tunning 가능성을 고려하여야 한다. 제어기 파라미터 값의 변경 가능 기능은 제어기 파라미터 변수를 공유 메모리 상에 위치시켜 두고 그 값은 운용자가 단말기를 통해서 변경시킬 수 있도록 구현하였다.

둘째, 제어 프로그램 변경이 가능토록 하여야 한다. 제어기 역시 고정되어 있지 않고 가변성을 가지므로 이에 대응할 수 있도록 제어 프로그램 변경시 HOST 컴퓨터에서 만들어진 object file을 공유 메모리와 공유 버스를 통하여 원하는 SLAVE 프로세서로 전송하는 기능을 구현하였다.

본 FTCS는 특히 flexibility와 extendibility에 역점을 두어 개발하였다. 이는 입출력 포인트 수의 증가및 제어 대상의 변화에 쉽게 대응할 수 있도록 하기 위함이다.

IV. 결론

본 연구는 화력 발전소 보일러 제어기의 신뢰도 향상의 한 방안으로 고장 진단및 back-up 제어 기능을 갖는 FTCS에 대하여 기술하였다. Fault Tolerant Control 분야는 최근에 관심이 기울어 지는 분야로 적용 사례가 부족함으로 인하여 성능 평가 기준이 부족한 실정이고 이는 앞으로 설치 운용을 통하여 유용한 기준들이 설정될 수 있으리라 전망된다.

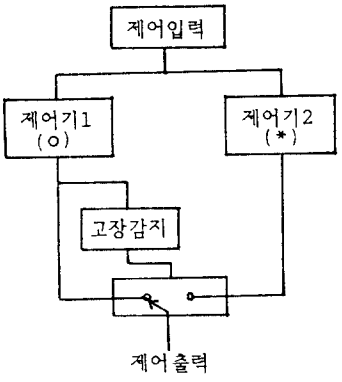
참고 문헌

[1] 이헌, "Fault Tolerant Computing Systems," 전자교환기술 제 1 권 제 1 호, 1985.

[2] 문봉채 외 3인, "FTCS의 Multi-processor 방식 적용에 관한 연구," 대한전기학회, 대한전자공학회 합동 하계학술회의 논문집, 1987.7.

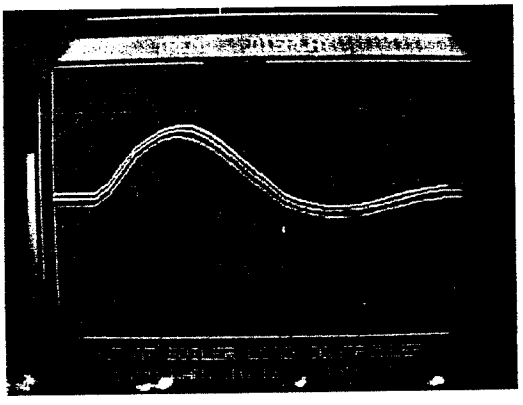
[3] 김지홍 외 3인, "발전소 보일러 제어기에 적용한 Fault Tolerant Control System의 연구," 대한전자공학회지 제 24 권 1 호, 1987.

[4] VMEbus Specification Manual, Motorola.

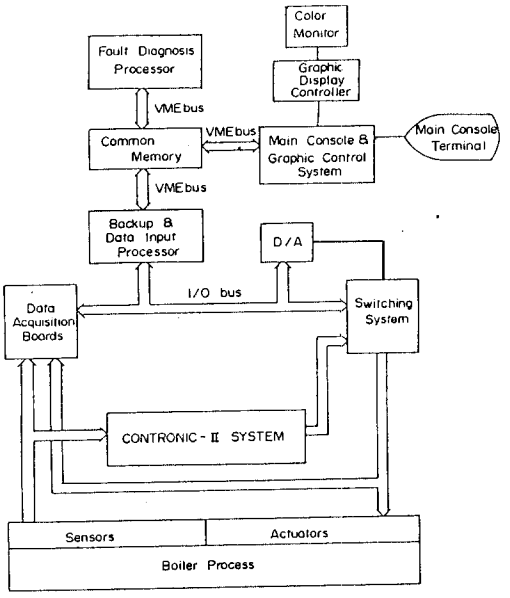


'*' : Standby 제어기
'o' : 동작중인 제어기

(그림 1) Standby 구조



(그림 2) Back-up 제어 응답



(그림 3) FTCS의 블록 선도