

# 발전소 보일러 제어기에 적용한 Fault Tolerant Control System의 연구

## (A Case Study on Fault Tolerant Control System for Power Plant Boiler Controller)

金志泓\*, 趙顯容\*\*, 鄭明振\*, 卞增男\*

(Jee Hong Kim, Hyun Yong Cho, Myung Jin Chung  
and Zeungnam Bien)

### 要 約

프로세스 제어기의 신뢰도 향상의 방안으로 Fault Tolerant Control System을 구성할 때의 고려 사항 및 발전소를 대상으로 FTCS의 적용에 대해 기술하였다.

아날로그 회로로 구성된 보일러 제어 시스템의 보수 유지 단계에서, 고장 탐지 및 진단기능, back-up 제어 기능을 구현한 마이크로 컴퓨터와 Bumpless Switching 시스템을 Add-on 시스템으로 추가하여 중복 구조를 갖는 FTCS를 구성하였다. IBM PC와 시뮬레이터를 이용하여 6개의 제어루프에 대해 소형 FTCS를 제작, 실험한 결과, 단위 고장에 대해 인위적 고장을 발생시키면 즉각 이를 탐지, back-up 제어로 전환하여 고장의 영향이 제거됨을 보였다.

### Abstract

As a means of improving the reliability of a process control system, a FTCS (Fault Tolerant Control System) is designed and applied to the boiler controller of a thermal power plant.

The proposed FTCS has capabilities of fault detection and diagnosis as well as back-up control and bumpless switching. A prototype of FTCS is implemented on an IBM PC as an add-on system and it is experimentally verified by using a boiler process simulator together with simplified analog controllers and a switching unit that an one-fold fault is detected in real time and back-up controller takes over the role of the original controller, controlling the faulty loop.

---

\*正會員, 韓國科學技術院 電氣 및 電子工學科

(Dept. of Elec. Eng., KAIST)

\*\*正會員, 韓國電氣通信公社

(O. A. SW. LAB., Korea Telecom.)

接受日字: 1986年 4月 3日

(※ 본 연구는 한국전력공사 기술연구원의 지원하에 수행된 협동연구의 일환임.)

### I. 序 論

최근 생산 시스템이 대규모화되고 복잡해짐에 따라, 자연적 또는 인위적 고장 요인에 의해 시스템이 원하는 동작을 못하는 경우, 그로 인한 파급효과가 막대할 수 있다. 예컨대 발전소의 경우 부분적인 고장이 발생 하더라도 전 시스템의 안정성을 위해 동작 정지를 유발시킴으로써 직접, 간접적으로 엄청난 손실이 발생된

다. 이런 추세에 따라 시스템의 신뢰성과 안정성의 향상에 대한 요구가 절실해지고 있다.

시스템의 신뢰도는 고장(fault)의 발생 빈도와 정도에 의해서 결정된다. 따라서 신뢰도 개선을 위한 연구는 고장의 원인을 분석하고 규명하여, 사전에 이를 예방하는 Fault Avoidance 방법과, 고장 발생시 그 영향을 최소로 줄여 시스템이 동작을 계속하도록 하는 Fault Tolerance 방법으로 나눌 수 있다. Fault Avoidance 방법은 경험 및 분석에 의해 적절한 소자의 선택, 환경 조절과 잡음 제거등의 방법에 의하나 고장을 완전히 방지할 수는 없고, 보다 적극적인 방법으로 Fault Tolerant System(FTS)을 구성하는 연구가 최근 많이 진행되고 있다.

현재의 FTS는 거의가 컴퓨터를 이용한 디지털 시스템에 응용되고 있으며,<sup>1,2</sup> 따라서 신뢰도 향상을 위한 연구 방향도 정보처리용, 제어용 Fault Tolerant Computing Maching의 설계와 개발이 추가되고 있다.<sup>3</sup> 미국 등지에서는 이를 이용하여, Hardware Redundancy를 이용한 FTMP(Fault Tolerant Multi-Processor)와 SIFT(Software Implemented Fault Tolerance) 방법을 상용 항공기의 제어 시스템에 응용하고 있다.

컴퓨터의 대중화와 Hardware Device의 저렴화로 인하여 Fault Tolerant Computer의 연구, 개발이 높은 수준에 이르렀으나,<sup>4</sup> 현재의 FTS의 대부분은 주기능이 Hardware Redundancy에 의해 이루어져 있다.<sup>5</sup> Hardware Redundancy의 구조는 여러가지로 분류할 수 있으나, 고장 탐지기능의 유무에 따라 SC(Self-checking), NSC(Non Self Checking) 구조로 양분할 수 있다. 대표적인 예로 TMR(Triple Modular Redundancy), Hot Stand-by, Cold Stand-by의 3종류가 널리 사용되며,<sup>6</sup> 항공 우주산업이나 원자력 발전소와 같이 고도의 신뢰도가 요구되는 곳에는 Highly Redundant System이 사용되기도 한다.

시스템 이론에 관한 연구에서도, 동적시스템에 대한 고장 탐지 및 진단에 관한 연구가 활발하며,<sup>7,8,9,10</sup> 대부분은 시스템의 정확한 모델링을 가정하고 state나 parameter의 추정 방법을 이용하여 고장 발생 결정, 고장 위치 및 정도의 감지를 행한다. 또한 multi-controller 구조에 의한 Fault Tolerance 기능을 부여하는 연구도 진행되고 있다.<sup>11</sup>

FTS의 연구는 대부분이 설계 단계에서 진행되고 있으며, 이미 설치된 시스템의 보수유지 및 신뢰도 향상의 일환으로 중복 구조를 첨가하는 연구는 거의 없는 상태이다. 일반 산업계에서는 Fault Avoidance 방법과 고장이 발생한 후에 경험과 현상 분석에 의하여 보수유지를 수행하는 소극적 방법을 취하고 있다. 그러나

발전소와 같이 초기 시설 투자가 크고 고도의 신뢰도가 요구되는 곳에서는 FTCS에 의한 신뢰도 향상의 연구가 시급한 것으로 사료된다.

본 논문에서는 보수 유지 단계에서 FTCS를 구성할 때의 기본 요건과 발전소에 응용한 FTCS의 설계를 제안하고, 이를 실험한 결과에 대해 검토, 기술하였다.

## II. FTCS의 구성시 고려사항

산업용 공정 제어기에 Fault Tolerance 기능을 부여하기 위해서는 일반 computing machine에 적용되는 사항외에도 주변 환경 및 프로세스의 특성이 고려되어야 한다. 우선 설계 단계에서 다음과 같은 사항이 고려되어야 한다.

1. Fault의 영향을 어느 정도까지 담당할 것인가를 고려한다.

예를 들면, 출력의 입장에서 단지 masking만 할 것인가, 혹은 고장을 탐지하여 여분의 시스템으로 전환하거나, 즉각적인 수리를 위해 고장 부위 및 고장정도까지 결정할 것인가에 따라 i) 항상 working하는 N modular redundancy, ii) 수리가 필요없는 large number of disposable spares, iii) 수리후 swiching-back을 위한 Dual Redundancy의 구조가 일반적으로 많이 사용되고 있다. 따라서 수리의 가능 여부도 중요한 요소로 대두되며, 항공 우주산업과 달리 산업 공정 제어 분야는 항상 운전자가 대기하며 수리가 가능한 상황이 대부분이다.

2. 프로세스의 특성을 파악한다.

특히, 연속공정(continuous process)의 실시간 제어기는 batch process 보다 시정수가 짧다. 따라서 제어기의 고장 발생시 프로세스에 영향을 줄 경우 즉각적인 대책을 위하여서는 고장탐지와 자동전환(Automatic switching) 시스템의 사양이 중요하다. 일반적으로 0.1초 미만의 프로세스 제어시는 fault masking 방법을 사용하여야 하며,<sup>12</sup> 기계적 시스템이나 유량, 온도 등의 제어에는 iii)의 구조를 사용한다.

3. 중복 구조시의 경제성을 고려한다.

규모가 커질 수록 동일 시스템의 복사에 의한 중복 구조시 비용이 상승하게 된다. 이 경우 하나의 중복시스템이 동시에 2개 이상의 시스템이 고장날 확률이 배제된 일군의 시스템을 back-up 하는 방안이 사용된다.

보수 유지 단계에서 기존의 설치, 운전중인 시스템의 신뢰도 향상을 위한 적극적인 방법으로 Fault Tolerance 기능을 부여할 경우는 동일 시스템의 사용 여

부가 고려되어야 한다. 특히 고장이 자주 발생하는 부분만 중복 구조를 구성하여 전체 시스템의 신뢰도 향상을 꾀할 수 있다. 또한 실제적인 계장시 입출력 신호의 측정 및 절환 작업이 간단하도록 구성하여야 하며, 첨가되는 시스템의 자체 신뢰도가 높아야 한다.

본 논문에서는 울산 화력발전소의 보일러 제어용 CONTRONIC II 시스템을 대상으로 중복 구조에 의한 FTCS를 설계하였다. CONTRONIC II는 70년대 아날로그 IC기술을 사용한 총 35가지 종류의 모듈로 구성되어 있고, 이를 조합한 360여장의 모듈이 보일러의 연료, 급수(feedwater), 연소공기, 온도 제어등 총 32개의 제어 루프를 형성하고 있다. 이와 같은 아날로그 제어기에 대해 동일한 시스템을 Add-on 시스템으로 선정, 중복 구조를 구성하는 것은 경제성 측면에서 불리하며 70년대 초반의 모듈은 생산 중지로 인하여 불량 공급의 어려움이 있다. 따라서 같은 제어 기능을 수행하는 디지털 제어기를 Add-on 시스템으로 선정하였다. FTCS의 고장 발생시 동작 기능을 보면, 기존 제어기에 의한 정상 동작중 고장이 발생하면 입출력 신호 분석에 의해 즉시 이를 탐지하고, 고장이 발생한 제어루프의 기능을 back-up 제어기가 담당하도록 switching 한다. 동시에 측정된 고장 현상을 이용해 고장 모듈의 위치와 고장 정도를 결정하여 운전자의 신속한 수리를 가능하도록 한다. 이때의 진행도는 그림 1과 같으며 back-up 제어기의 성능에 따라 동시에 몇개의 고장난 제어 루프를 대체할 수 있다가 결정된다. 이와 같은 기능을 위해 제안한 FTCS의 블록 선도는 그림2와 같으며, III장에서 소형 proto-type에 의한 실험으로 본 설계의 타당성을 보였다.

III. 발전소 보일러 제어기에 대한 FTCS의 적용

1. FTCS의 구성

대상 시스템인 울산 화력발전소는 관류형 보일러를 사용한 대용량(400MW)의 발전소로, 제어 시스템의 고장에 기인한 사고가 전체 사고의 35.1%를 차지하고

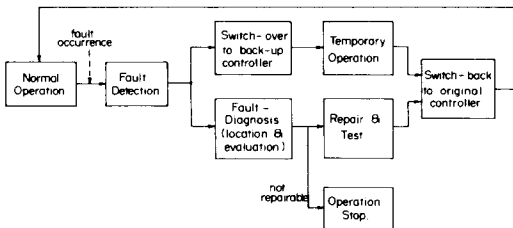


그림 1. FTCS의 진행선도  
Fig. 1. Flower diagram of FTCS.

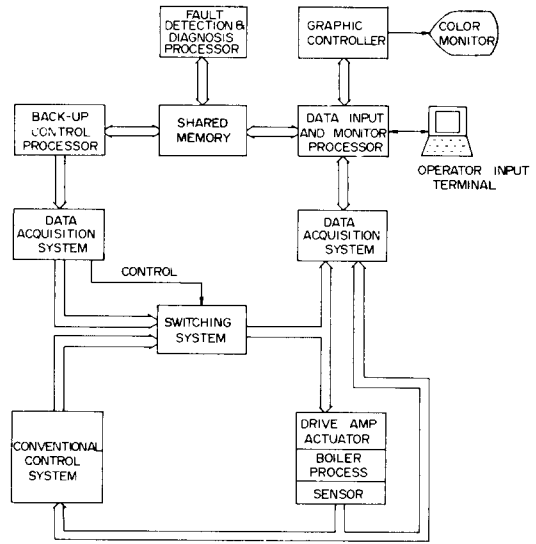


그림 2. FTCS의 블록선도  
Fig. 2. Block diagram of FTCS.

있어 제어 시스템의 고신뢰화가 시급한 연구 과제로 요구되고 있다. 보일러 부하 제어부는 기능에 따라 총 32개의 단일 루프로 구성되어 있으며 대표적인 것으로는 부하 명령에 따라 연료(중유)의 유량을 조절하는 밸브 제어, 연소 공기의 양을 조절하는 Damper 제어, 급수의 압력과 유량을 조절하는 펌프출력 제어, Super-heater, Reheater 등 각 부분의 온도 제어, 기타 수위 제어 등이 있다. 한 예로 연료의 유량제어기의 블록선도는 그림 3으로 나타나며 Plant 1은 펌프 출력에 대한 압력의 변화, Plant 2는 압력 변화에 따른 총 연료의 유량 변화의 특성을 가지며 입력은 부하에 따른 연료의 요구량, 상태변수  $x_1$ 은 압력,  $x_2$ 는 유량을 나타낸다. 이 같은 제어기들은 PI제어기, PD 제어기 등이 대부분이며 서로 유사하거나 각 층별로 동일한 기능을 갖기 때문에, 효과적인 back-up 제어를 할 수 있다. 보일러 제어에 쓰이는 CONTRONIC II 중에서 FTCS의 back-up 제어 대상 부분은 그림 4의 Central operation unit로서 외부의 신호는 0~3V를 사용한다. IBM PC를 이용한 소형 FTCS의 구성도는 그림 5와 같다. Switching 시스템은 power fail시에 원래의 제어기가 작동하도록 기계적 릴레이를 사용하였고, switching전후의 신호차에 의한 급격한 변동으로부터 프로세스를 보호하기 위해 Bumpless transfer 회로를 각 릴레이마다 설치하였다. Bumpless transfer 회로는 그림6과 같다.

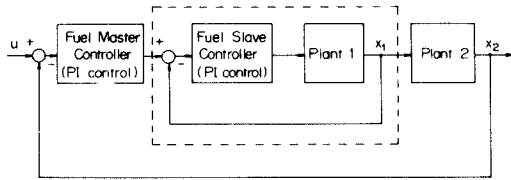


그림 3. 연료유량 제어블록선도  
Fig. 3. Block diagram of fuel flow rate control.

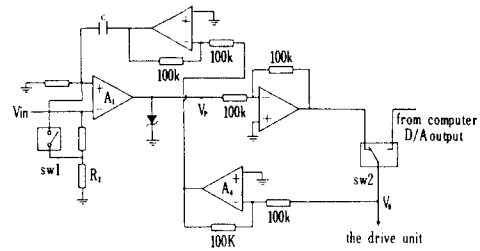


그림 6. Bumpless transfer 회로  
Fig. 6. Bumpless transfer circuit.

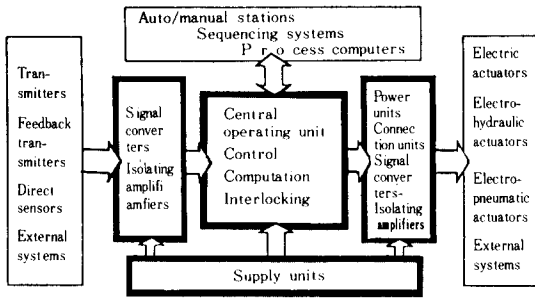


그림 4. Contronic II system  
Fig. 4. Contronic II system.

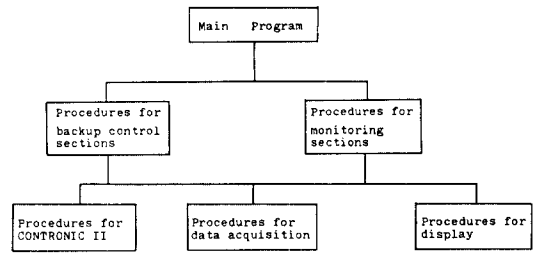


그림 7. 소프트웨어의 구성도  
Fig. 7. Software block diagram.

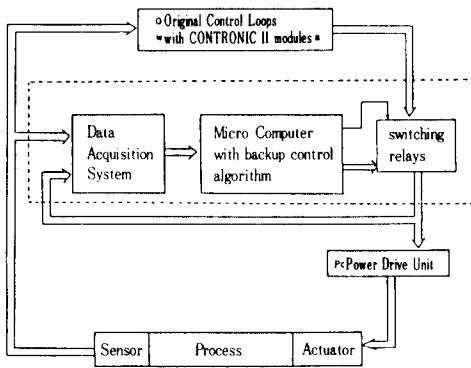


그림 5. 하드웨어 블록선도  
Fig. 5. Hardware block diagram.

소프트웨어는 그림 7 과 같은 procedure로 구분할 수 있다.

원래의 제어가 CONTRONIC II 의 여러 종류의 모듈의 조합으로 구성된 것처럼 프로그램의 구성에서도 각 모듈에 해당하는 subroutines을 사용함으로써 프로그램의 양을 줄이고 다른 제어 알고리즘에 적용이 용이하도록 하였다. 한 예로 Fuel Oil과 Combustion Air

의 제어 등에 쓰이는 PI unit(모듈 이름 CT032)의 디지털 PI 알고리즘은 식 1 과 같으며 anti-reset windup 기능을 첨가하여 velocity form으로 고쳐서 PASCAL 언어로 구현한 프로그램은 그림 8 과 같다.

$$m_n = \frac{100}{X_p} \left( e_n + \frac{T}{T_n} \sum_{k=0}^n e_k \right) + m_0 \quad (1)$$

- $m_n$  : manipulated variable at step n
- $e_n$  : error value at step n
- $X_p$  : proportional band [%]
- $T_n$  : integral time constant {sec}
- $T$  : sampling period {sec}
- $m_0$  : output bias

이와 같은 각 subroutine은 Monitoring section과 Back-up control section에서 각 제어 알고리즘 마다 지정된 순서대로 수행된다.

Monitoring procedure는 Data Acquisition과 Display를 수행하며 각 프로세스 값들을 이용해 제어 알고리즘에 따라 출력값을 산출한다. 이를 측정된 출력과 비교하여 그 오차가 주어진 Tolerance 값을 초과하면 고장으로 판명하여 고장난 부위에 대하여 스위칭한 후 back-up 제어를 수행하도록 한다. 이와 같은 구조는 중복제어의 대상 제어 루프가 증가할 때 쉽게 확장

```

procedure PI(v1, v2, v3, v4:real;var py:real); {PI unit}
var
  pe:real;
begin
  pe:=v1+v2+v3+v4;
  py:=py+(100.0/Xp)* (pe-pe1+T*pc/Tn);
  if py>1.0 then py:=1.0 else if py<0.0 then py:=0.0;
  pe1:=pe;
end;
    
```

그림 8. PI unit의 Subroutine  
Fig. 8. Subroutine of PI unit.

할 수 있으며, 고장 탐지, back-up 제어, 데이터 입력과 Display 기능을 분리할 때 쉽게 구현할 수 있다. Sampling time은 각 제어 알고리즘별로 표 1과 같이 정하였고, 이는 IBM PC의 computing power와<sup>13)</sup>의 guide를 고려하여 정하고 IBM PC의 PASCAL에 내장된 function인 "tics"를 이용, 구현하였다.

표 1. 각 제어 loop의 sampling period  
Table 1. Sampling period of each control loop.

Section name	Function	Sampling period(sec)	minimum possible sampling period
LOAD 1	Fuel Demand Generation	0.306	0.1(sec)
LOAD 2	Possible Load Check	1.0	0.3(sec)
FUEL 1	Fuel Control(master)	0.306	15(msec)
FUEL 2	Fuel Control (slave, each stairs)	0.306	15(msec)
AIR 1	Combustion Air Control (Master)	0.306	0.12(sec)
AIR 2	Combustion Air Control (slave, each stairs)	0.306	15(msec)

2. 실험 및 분석

본 FTCS의 실험을 위하여 CONTRONIC II 시스템과 보일러 프로세스의 시뮬레이터를 제작하였다. 시뮬레이터와 FTCS를 Integration하여 구성한 시스템은 그림 9와 같다. CONTRONIC II의 시뮬레이터는 주요 기능만 간략화한 아날로그 회로로 구성하였고, 인위적인 하드웨어 고장이 가능하도록 하였다. 보일러의 열역학적 특성은 복잡한 비선형 시스템이므로, 운전시 데이터를 중심으로 간단한 선형 1차 시스템으로 구현하였다.<sup>17,21)</sup> 밸브나 펌프 등의 모델링은 Ziegler-Nichols의 Tuning Rule중 Transient Response Method를 이용하여 PI 제어기의 이득 상수로부터 역산에 의해 구하였다.<sup>12,23)</sup> 실제로 밸브나 펌프 등은 동적 특성에 대

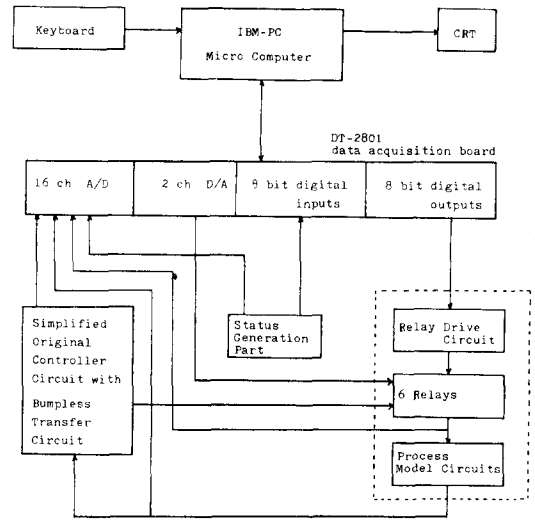


그림 9. 실험 시스템의 구성도  
Fig. 9. Hardware block diagram of experimental system.

한 정보가 없는 상태에서 운전자가 출력 응답만 보며 경험적으로 제어 이득 상수를 조절하였으므로 Plant를 1차 지연 시스템으로 하여 역산에 의해 Plant의 모델링을 하였다. 그림10은 원래의 제어기와 Back-up 제어기를 임의로 switching 할 경우의 제어 입력(실선)과 프로세스의 출력값(점선)을 나타낸다. 그림 11은 12초 경과후 인위적 고장을 발생시켰을 때 이를 탐지, back-up제어를 수행함을 보여 준다.  $t_1$ 은 고장 발생시간,  $t_2$ 는 back-up제어로 switching된 시간을 나타내며,  $t_2-t_1$ , 즉 제어 기능이 걸려된 시간을 최소화함으로써 고장의 영향을 최소화하는 FTCS의 성능을 나타낼 수 있다. 실험에 사용한 IBM PC의 계산 능력

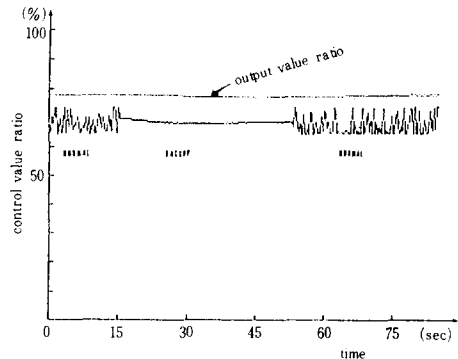


그림10. Air2 section의 control 전환  
Fig. 10. Switching of control in Air 2 section.

상, 6 개의 제어 루프를 모니터링하여 고장을 감지하는 시간은 1 초로 나타났으며, 이는 계산 능력이 뛰어난 마이크로 프로세서를 사용함으로써 더욱 줄일 수 있다. 이외에 고장으로 기인된 출력의 변화율의 최대치, 고장 탐지의 정확도와 back-up 제어기와 switching 시스템의 자체 신뢰도, 동시에 발생한 고장을 몇개까지 탐지, back-up 할 수 있는가의 정도, 운전자의 신속한 수리 후 switching back하는 시간(그림11의  $t_3$ ) 및 이를 위한 진단 정보의 제공 등으로 FTCS의 성능을 나타낼 수 있으며 이를 정량화하거나 이론적 방법을 제시하기 위해 많은 연구가 필요하다.

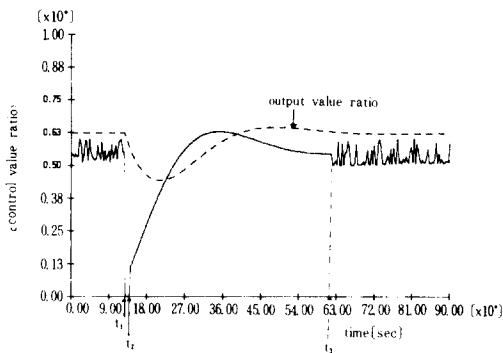


그림11. FTCS의 back-up 제어동작  
Fig.11. Back-up control of FTCS.

V. 結 論

기존 시스템의 보수유지 단계에서 고신뢰화를 위한 방안으로 중복 구조의 제어기를 추가 설치함으로써 Fault Tolerance 기능을 부여하였다.

특히, 대규모의 이산로그 회로로 구성된 발전소 보일러 제어 시스템에, 마이크로 컴퓨터를 사용하여 디지털 프로세스 제어 기술을 적용함으로써, 종래의 단순 복제 방법보다 비용이 월등히 저렴해지고 효율적인 중복제어기를 설계하였다. 이를 위하여 bumpless transfer 기능을 갖는 Switching system과, 제어 시스템 및 프로세스의 하드웨어 시뮬레이터를 제작, IBM PC를 이용한 중복제어기와 결합하여, 6 개의 제어 loop에 대해 실험을 수행한 결과, 인위적 고장발생시, 즉시 이를 탐지, 고장난 부분을 대신하여 동일한 성능의 back-up 제어를 수행함을 알 수 있었다.

일련된 연구 과제로써 발전소 보일러 제어시스템 전체를 대상으로 Multi-processor에 의한 FTCS를 개

발하여, 이를 발전소에 직접 적용, 운용함으로써, 발전소의 신뢰도 향상에 기여하는 연구가 수행될 것이며, 이에 대한 시도가 전후한 국내에서도 신뢰도 개선에 관한 연구가 활성화되어야 할 것이다.

參 考 文 獻

- [1] A. Avizienis, "Fault tolerant systems", *IEEE Trans. on COMPUTERS*, vol. c-25, no. 12, pp.1304-1311.
- [2] D.A. Rennels, "Fault-tolerant computing-concepts and examples", *IEEE Trans. on Computer*, vol. C-33, no. 12, Dec. 1984. pp.1116-1129.
- [3] J.H. Wensley, "Fault tolerant techniques for power plant computers", *IEEE Trans. on PAS*, vol. PAS-101, no. 1, pp. 100-105, Jan. 1982.
- [4] K. Asami, K. Yanai, T. Ito, *Super-high Reliability Fault Tolerant system NUREC-3000*, IECON' 84, pp. 1181-1184.
- [5] "Fault Tolerant Computing, System", pp.46-61.
- [6] A.J. Laduzinsky, *Fault Tolerant Control Means Never Having to Say You're Sorry*. Control Engineering, pp. 71-74, Feb. 1985.
- [7] P.J. Cleuand, P.L. Sank, *Power Plant Control -an overview* Joint Automatic Control, voA3-A, 1976.
- [8] L.A. Mironovskii, "Functional diagnosis of dynamic systems" *Translated from Avtomatika i Telemekhanika*, no. 8 pp. 96-121, 1980.
- [9] R. Inermann, "Fault detection method for the supervision of technical process", *Process Automation*, vol. 1, pp. 36-44, 1981.
- [10] R. Isermann, "Process fault detection based on modelling and estimation methods-A survey", *Automatica* 20, pp. 387-404, 1984.
- [11] A.S. Willsky, *A Survey of Design Method for Failure Detection in Dynamic Systems*. Automatica 12, pp. 601-611, 1976.
- [12] T. Nishiyama, "Prevention and detection of failures in thermal power plants", *Thermal and Nuclear Power*, vol. 29, no. 10. pp. 77-106, 1979.
- [13] Smith, *Digital Computer Process Control*,

- INTEXT Educational Publishers, 1972.
- [14] Astrom, Witten mark, *Computer Controlled System*, prentice Hall, 1984.
- [15] F. Hagedorn, Dr. G. Klefenz, "H & B power station Control", H&B monograph 3587 EN
- [16] 울산화력 발전소 4, 5, 6호기 운전조작 설명서, 대우엔지니어링, 1980.
- [17] 조현용, "화력 발전소를 대상으로한 백업 컨트롤 시스템의 연구" KAIST 석사 학위논문, 1986.
- [18] 문봉채, "선형동적시스템에서의 고정진단 알고리즘" KAIST 석사 학위논문, 1986.
- [19] D.D. Siljak, "Reliable control using multiple control system", *Int. J. Con.*, vol. 31, no. 2, pp. 303-329, 1980.
- [20] W.F. McGill, S.E. Smith, "Fault tolerance in continuous process control", *IEEE MICRO*, vol. 4, no. 6 Dec, 1984, pp. 22-33.
- [21] 어재용, "관류형 보일러의 비선형 저차모델 개발에 관한연구" KAIST, 1986.
- [22] Ziegler, J.G. and N.B. Nichols, *Optimum Settings for Automatic Controller*. Trans. ASME, 64, pp. 759-768, 1942.
-