PLC 제어 시스템의 신뢰도 향상에 관한 연구

(A Study on the Enhancement of Reliability for PLC Control System)

이석용* · 이홍규

(Sok-Yong Lee · Hong-Kyu Lee)

한국 기술 교육 대학교 전기·전자 공학과

(Dept.of Electrical & Electronic Eng.. Korea University of Technology and Education)

Abstract

In many fields of automation, increasingly high demands are being placed on the availability and fault tolerance of programmable logic controller(PLC). Particularly in fields where a plant shutdown would be extremely expensive. In such cases, only redundant systems can offer the standard of availability required. The redundant configurations contain more then would normally be necessary for the relevant function. Fault tolerant systems will normally continue to operate even if one or more faults cause parts of the control system to fail.

1. 서 론

현재 생산합리화 및 성력화를 위해 생산시스템의 자동화가 많이 추진되고 있다. 컴퓨터 및 그 기술을 도입함으로써 제어기술이 발전되고 생산 시스템의 자동화는 진전되어 왔다. 최근들어 각종 산업현장의 자동화 설비에 대부분 PLC(programmable logic controller)를 사용하여 제어하고 있으며, 그 기능과 특성이 점차 발전하면서 그 응용 범위도 확대되어 가고 있다. 따라서 PLC의 용도가 확대되면서 제어 분야에서의 고도화와 복잡화 그리고 안전화를 요구하고 있으며 자동화와 성력화 및 무인화의 가장 효과적인 수단으로써 광범위하게 사용되고 있다. PLC를 적용하여 각종 설비의 제어를 통한 작업 환경 개선으로 작업 능률을 높이고 생산성의 증대를 가져 올 수 있다. 특히 연속 공정, 위험 지역에서의 적용은 예를 들면 화학 공정, 발전소, 제련, 제강, 소성 설비, 공항 등의 제어용 PLC 고장 사고는 중대 재해를 유발한다. 이러한 중대 재해를 예방하기 위하여 고장허용 제어 시스템을 적용하여 연속적인 운전을 할 수 있다. 이 고장허용 제어 시스템은 PLC나 주요 요소(입력, 출력)에서 하나 혹은 많은 고장이 발생한 경우에 전체 공정의 중단 없이 연속적으로 운전하는 것이다. 따라서 고장허용 제어 시스템은 전체 제어 시스템의 고장에 대해서 신뢰도를 확보하는 것이다. 여기에서 고장허용 제어 시스템을 적용 시에 경제적인 비용은 두가지 측면에서 고려 되어야 할 것이다. 첫 번째로는 고장이 발생한 경우에 많은 생산량의 손실을 가져오는 경우(예를 들면 조립 생산라인 등), 두 번째로는 고장 시에 따른 적은 생산 손실이라도 주위의 공정에 막대한 영향을 미치는 경우 또는 복구 및 손실 비용이 많은 경우(예를 들면 프로세서 공정 등)로 분류할 수 있다. 따라서 고장허용 제어 시스템은 생산 공정의 연속적인 운전과 손실을 방지하고 고장 발생 시 시스템의 중단 없이 수리가 가능하게 하고, 제어 시스템의 신뢰도를 향상시킨다.

1.1 PLC 제어 시스템

일반적인 경우의 PLC는 마이크로프로세서를 기반으로 하는 제어기로서, 어느 샘플링 순간에서 이진수 입력신호의 값을 받아들여 프로그램 실행동안의 지연 시간을 가진 후, 이진 출력 신호의 값을 갱신하여 출력한다. PLC의 한 주기 또는 한 스캔(scan)은 한 번의 입력값의 샘플링, PLC의 내부 레지스터의 값을 계산하여 갱신하는 프로그램 실행, 그리고 새로운 출력 신호의 기록등으로 구성되어진다. 이러한 PLC의 동작을 수식으로 표현하면 다음과 같다.

$Q(k) = P(Q(k-1), U(k))$

여기서, $Q = (q_1\ q_2\ \ldots q_n)$

단, n은 state 변수의 개수

$Q(k)$: k번 스캔후의 state 변수들의 값

$U = (u_1, u_2, \ldots, u_l)$

단, l는 입력 신호의 개수

$U(k)$: k번 스캔 후의 입력 변수들의 값

단, $k \geq 1$이고, $Q(0)$는 초기 state로 주어진다.

P :state 변환 함수

1.2 PLC 제어 시스템의 고장과 예측

PLC 제어 시스템의 신뢰도, 가용성(Availability) 안전성 항목은 언제나 명백하지 않으며, 때때로 에러(error)를 불러일으키기 쉽다. 신뢰도는 모든 측정에서 고장이 발생되지 않았다고 해서 그것이 100(%)의 신뢰도를 갖는 것은 아니며 고장율 (λ)은 신뢰도의 측도 이다. 여기서 고장율은 다음과 같이 표현할 수 있다.

$$\text{고장율}(\lambda) = \frac{n}{N \times t}$$

단, n:시간 t 동안의 고장수 N:나머지 구성요소

1.3 제어 시스템의 고장 특성

PLC 제어 시스템에서 고장의 분포도는 그림1과 같으며 경험적으로 볼 때 PLC를 설치함에 있어 고장은 다음과 같이 개략적으로 분산시킬 수 있다. PLC 부분에서의 고장은 전체 고장의 5(%) 정도 발생한다. 그러나 고장율은 적지만 고장 시 엄청난 손실을 가져 올 수 있다. 입, 출력 모듈은 90(%)로써 전체 고장의 40(%)에 해당한다.[5]

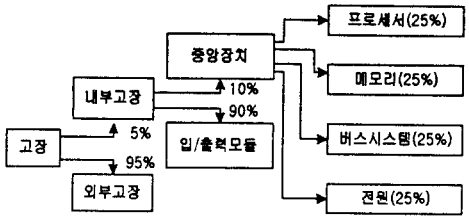

그림 1. PLC 설치에서의 고장발생 분포도
Fig 1. distribution diagram of fault about PLC

PLC의 가용성은 임의 시점(any point of time)에 시스템 또는 장치가 효과적으로 동작할 확율이며 다음과 같은 측도를 사용한다.

즉, 가용성(A) =MTBF/(MTBF+MTTR)

MTBF(mean time between failure): 고장간 평균 시간

MTTR(mean time to failure): 평균 고장 시간

여기에서 가장 이상적인 가용성은 A= 1 이지만 이 경우는 항상 잔여 하는 고장 가능성 때문에 실제로는 이루어 질 수 없는 경우이다. 그러나 votor 시스템을 사용함으로써 이러한 이상적인 상태에 근접하게 도달 할 수 있으며 스탠바이 시스템, 3중에서 2 선택하는 시스템 ,상호 검색 기능을 가진 다중 채널 등을 적용하여 시스템의 가용성을 증대시킬 수 있으며 본 논문에서는 2 채널 (1-out-of-2) 스탠바이 시스템인 이중화 시스템을 적용하여 시스템의 가용성을 높일 수 있는 방법을 연구하였다.

PLC의 신뢰도는 이중화 모듈을 사용하여 MTBF를 연장 할 수 있으며 1 채널 시스템(1-out-of-1)을 기준으로 하여 2 채널(1-out-of-2) 시스템에 대한 신뢰도를 계산할 수 있다.

$$MTBF_{1002} = \frac{MTBF_{1001}^2}{2MDT + 2(1-dc).MTBF_{1001}}$$

단. dc(diagnostic coverage)=약 95(%)

MDT(mean down time): 에러 발견 시간 및 수리에 소요되는 시간 또는 고장난 모듈의 교체에 소요되는 시간

따라서 결국 이중화 시스템의 MTBF는 MDT에 의해 결정되어 진다.

그리고 PLC 모듈의 신뢰도에 대하여 보통 PLC 구성품의 MTBF는 다음과 같이 표현 할 수 있으며 CPU(central processing unit)는 약 15년 그리고 입력 및 출력 모듈은 약 50년 정도이다.[3]

1.4 PLC의 시스템 구성에 따른 MTBF의 비교

PLC의 시스템 구성에 따른 MTBF을 비교하기 위하여 초기 조건을 다음과 같이 가정한다.

가정: ① MDT: 4시간
② 주위 온도: 40℃
③ 버퍼(buffer) 전압 : 정상적인 상태
④ 1-out-of-1 시스템을 표준 시스템으로 하고 이때의 MTBF를 1 로 가정한다.

1) 스프리트 마운틴 랙(split mounting racks)을 사용한 CPU 이중화 시스템 구성 방법인 경우의 MTBF는 23배이고 분리된 마운틴 랙을 사용한 경우의 CPU 이중화 시스템의 MTBF는 59배이다.[3]

2) 입, 출력 모듈을 분리한 경우의 시스템 구성[3]

기준: 1 채널 이중화 CPU, one-sided 혹은 분산형 입, 출력 모듈을 사용한 경우의 MTBF를 1로 가정한다.
① 이중화 CPU, 분산형 스위칭 입, 출력 모듈인 경우 MTBF는 3배이다.
② 이중화 CPU, 분산형 스위칭 입, 출력 모듈인 경우 MTBF는 65배이다.
③ 이중화 CPU, 분산형 스위칭 입, 출력 모듈인 경우 MTBF는 70배이다.

PLC 제어 시스템의 고 신뢰도를 실현하기 위한 기본 요건은 고장회피(fault avoidance) 기술과 고장허용(fault tolerance) 방법을 사용한다. 여기에서

고장 회피법은 아주 높은 신뢰도를 갖는 부품을 사용하여 고장 발생 확율을 줄임으로써 시스템의 신뢰도를 높이는 방법이다. 그런데 이 방법에는 개별 부품의 신뢰도에 따른 고장 발생 확율을 가지고 있으므로 부품별 고장에 따른 기기의 고장이 발생되고 이로 인하여 전체 시스템의 신뢰도가 저하되고 시스템의 안정성을 해치게 되어 가용성을 감소시키게 된다. 그리고 고장 허용법이란 어떤 시스템의 기기나 부품이 고장 났을 경우에도 신속히 적절한 조치를 취함으로써 전체 시스템을 계속 적으로 정상 동작하도록 하고 시스템의 신뢰도를 높여서 가용성 및 안전성 그리고 연속 운전을 얻는 방법이며 고장 검출과 고장 격리 그리고 고장 조치 등의 3 단계로 구성된다 즉 ① 고장을 일으키지 않도록 하는 것 ② 고장의 검출 및 진단이 정확하게 실현 될 것.(고장 진단)③ 고장의 수리 및 복구가 단시간에 확실하게 실행 될 것.(고장 복구) ④ 고장의 영향을 받지 않고 운전이 가능 할 것.

①은 고장 회피(fault avoidance) 기술이며 ②에서 ④까지는 고장허용 기술(fault tolerance)이다. 본 논문에서는 고장의 영향을 받지 않고 연속 운전이 가능한 이중화 시스템을 적용하고자 한다. 실시간으로 제어 대상 계의 시뮬레이션을 실시하고 또한 PLC 고장 허용에 대한 이중화 제어 시스템의 실례를 소성로(燒成爐.kiln) 제어 시스템에 적용하여 각종 고장을 모델로 하여 본 방법의 실용성에 대하여 논술하고자 한다.

1.5 PLC 고장 허용 제어 시스템의 구성

PLC 고장 허용제어 시스템의 이중화 구성 방법은 CPU 모듈, 입, 출력 모듈, 네트워크의 이중화를 통하여 이중화 시스템을 구현 할 수 있다.

2. 본 론

2.1 CPU 모듈의 이중화

2대의 CPU가 병렬 운전 중 마스터 CPU의 고장 발생 시 스탠바이 CPU가 제어의 중단 없이 마스터로 연속 운전된다. 또한 스탠바이 CPU 상태로 전환되며 2대의 CPU가 동일 프로그램을 동시에 수행하므로 마스터에서 스탠바이, 스탠바이에서 마스터로 운전이 될 때 시간 지연이 발생하지 않고 연속 운전된다.

2.2 입, 출력 시스템의 이중화

입, 출력의 이중화는 입, 출력부의 고장에 의한 부하 운전 정지를 예방하고 연속 운전을 한다. 여기서 입, 출력 모듈의 선정 시에는 다음 사항을 고려하여야 한다.

1) 입출력 모듈의 특성에 따라 지연 시간이 다르므로 원하는 응답 시간을 고려하여야 하며 이것은 이중화 시스템 구성 시에 설계 단계에서부터 고려되어야 한다.
2) 입력 모듈은 입력 전압에 유의하여 선정되어야 한다.
3) 출력 모듈의 정격 개폐 용량을 초과하지 않는 범위 내에서 사용해야 한다.
4) 부하에 인가되는 전압이 교류, 직류에 따라서 출력 모듈을 보호할 필요가 있으며 교류 전원 계통의 유동성 부하 즉 예를 들면 솔레노이드 부하나 역율이 낮은 부하인 경우는 SSR(solid state relay) 출력 모듈을 사용하며 릴레이 출력 모듈을 사용하는 경우는 모듈의 수명이 단축된다.

2.3 통신 시스템의 이중화

상위 컴퓨터와 CPU와 입출력 모듈간의 이중화 네트워크를 구성한다.

2.4 전원 모듈의 이중화

CPU, 입. 출력. 인터페이스, 특수 기능 모듈에 그리고 중설 유니트 및 네트워크에 접속되는 리모트 베이스에 공급되는 전원을 이중화한다.

2.5 시뮬레이션용 PLC 고장허용 제어 시스템의 이중화 구성

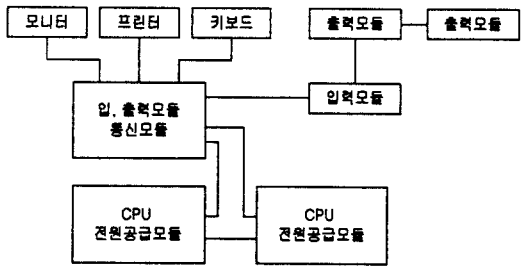

그림 2. PLC 고장허용 제어 시스템 구성 (하드웨어)
Fig2. configuration onthe fault-tolelrant control of PLC

상기에서 언급한 이중화 시스템을 고려하여 PLC의 고장에 대비한 고장 허용 제어용 이중화 시스템을 그림2와 같이 구성하여 시뮬레이션 하였으며 여기에 사용된 PLC 모듈은 SIMATIC S5을 사용하였고 적용 설비는 실제 PLC 고장 허용 제어 시스템으로 연속 운전이 필요한 소성로(燒成爐 . kiln) 제어 시스템에 적용하여 1-out-2 PLC 시스템

로 전환되며 마스터 CPU는 계속 운전되어지고 스탠바이 CPU는 에러 발견 모드로 전환되고 이때의 통신은 불가능하다.

③ 스탠바이 CPU가 완전히 자기 테스트를 끝낸 결과 에러를 발견한 경우는 스탠바이 CPU는 고장모드로 전환되고 마스터 CPU는 계속 운전된다.

④ 스탠바이 CPU가 완전히 자기 테스트를 끝낸 결과 에러를 발견하지 못 한 경우 스탠바이 CPU는 다시 링크업(link-up)과 update 모드로 된다. 그리고 운전 시스템은 마스터와 스탠바이 상태로 운전된다.

2.9 이중화 모드와 전환 관계

이중화 모드의 전환 과정은 그림5와 같으며 운전 상태에 따라서 단독 모드, 스탠바이 실행, 에러 발견 모드, 이중화 모드로 전환된다.[1]

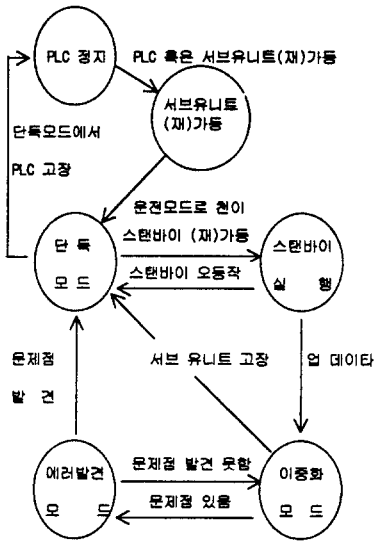

그림5. 이중화 모드와 전환 관계
Fig5. Redundant modes and transitions

2.10 유저(user) 프로그램에서 이중화 입, 출력 모듈의 전환 관계

이중화 입, 출력 모듈에서의 고장 허용 운전에 대해서 전환 관계는 그림6과 같고 여기에 사용되는 알고리즘은 다음과 같다.

(1) 입, 출력 모듈의 이상 유무를 OB1을 호출하여 체크한다.

(2) 입, 출력 모듈에서 에러가 발생하면 OB 122를 호출한다.

(3) 모듈에서 에러 발생시 에러 발생이 셋트된다.

(4) 입, 출력에서 DB5.DBX 0.0와 DB5.DBX 0.1을 호출한다. (DB : data block)

(5) 만약 모듈에서 고장이 발생한 경우 고장허용 상태 (연속 운전 상태)에서 모듈을 교체하고자 할 경우에는 OB 83을 호출하여 프로그램을 실행시킨다.

3. 실험 및 결과 고찰

PLC 고장 허용에 대한 이중화 제어 시스템의 하드웨어 구성은 그림2와 같이 실시하였고 실험에 사용된 구성품은 다음과 같다.

1) 실험에 사용된 PLC 제어 시스템 : SIMATIC S5, (전원 모듈, CPU, 입, 출력 모듈, 통신 모듈, 인터페이스 모듈)
2) 프로그래머 : PG 720
3) 실험에 사용된 시스템 소프트웨어 : COM 155H, STEP 5
4) 실험에 사용된 유저(user) 프로그램은 OB, FB, DB, PB, SB 이며 실험 조건에 적합하게 작성하였다.[2][4]
   OB : organization block FB : function block
   DB : data block PB : program block
   SB : sequence block

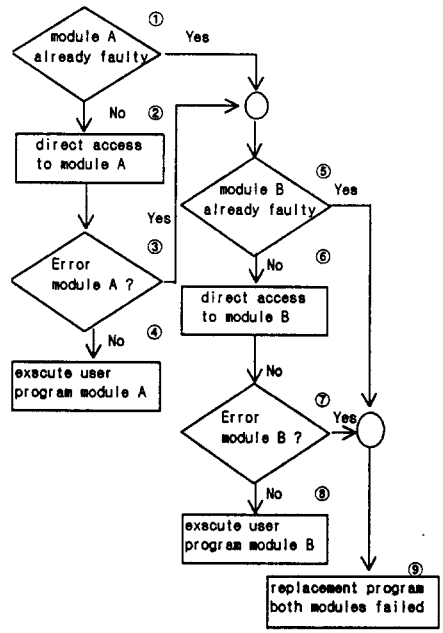

그림6. 이중화 입, 출력 모듈에서 프로그램 실행 관계
Fig6. Execution of program in the reduandant I/O module

의 이중화 노드 표현 방법, 이중화 시스템에서 시스템 모드와 운전 모드의 관계, 에러(error) 발견 모드, 이중화 시스템에서 고장 허용 연속 운전으로 천이(遷移)되는 과정, 유저(user) 프로그램에서 이중화 입, 출력 모듈의 전환 관계, 프로그램 실행 관계 그리고 천이(遷移)에 필요한 소프트웨어 구성과 PLC제어 시스템의 고장 시에 마스터 와 스탠바이 시스템과의 실행 및 연속 운전에 대하여 논술하고자 한다.

2.6 1-out-of-2 PLC 시스템의 이중화 노드 (node) 표현 방법

PLC의 이중화 노드 표현 방법으로는 오동작이 없는 상태 즉 정상적인 운전 상태에서의 네트워크를 구성하는 방법에서 오동작이 발생하여 고장 허용 제어 노드와 전체 고장으로 시스템이 정지되는 과정을 노드로 표현하면 그림3과 같다.[3]

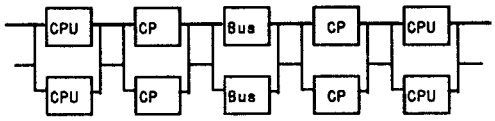

그림3-a 오동작이 없는 경우의 이중화 네트워크 구성

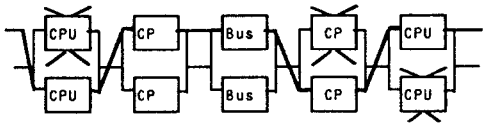

그림3-b 이중화 네트워크 상태에서 오동작이 발생되어 공장 허용 시스템으로 연속 운전이 되는 상태 노드

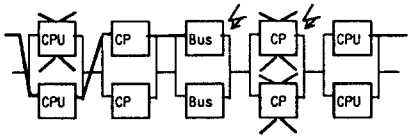

그림3-c 1-out-2 시스템 네트워크 상태에서 전체 고장 노드

그림3. 1-out-of-2 PLC 시스템의 이중화 노드 표현
Fig3. Redundancy node a 1-out-of-2 PLC system

2.7 이중화 시스템의 시스템 모드와 운전 모드의 관계

PLC의 이중화 시스템에서 마스터 CPU와 스탠바이 CPU 간의 시스템 모드는 전원 공급에서부터 이중화 시스템 모드는 정지, 가동, 단독, 링크업, update, 이중화 모드 등으로 구별할 수 있으며 각 모드에서의 마스터 CPU와의 운전 관계는 다음과 같이 진행된다.

① 이중화 시스템에 전원이 공급되면 두 개의 마스터, 스탠바이)는 정지 모드로 된다.
② 마스터 CPU는 가동되고 OB 100, OB102로 진행된다. (여기서 OB : organization block)
③ 마스터 CPU가 가동이 완료되면 마스터 CPU는 단독 모드로 전환되고 운전된다. 스탠바이 CPU가 link-up을 요구하면 마스터 CPU에서 스탠바이 유저(user) 프로그램을 스탠바이 CPU로 up-date 한다.
④ 링크 업(link up)이 완료되면 스탠 바이 CPU는 스캔 싸이클 (scan cycle) 상태로 운전된다.
⑤ 마스터 CPU와 스탠바이 CPU는 up-date에 따라 운전 상태는 되고 2개의 CPU는 이중화 모드로 동기화 운전을 한다.

2.8 에러(error) 발견 모드

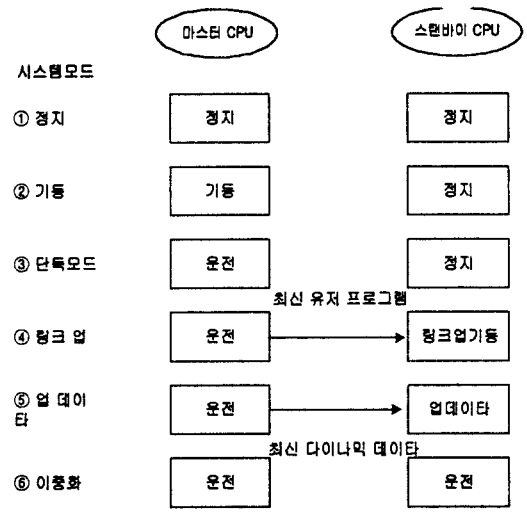

그림4. 이중화 시스템의 시스템 및 운전 모드 관계
Fig4. System and operation modes of the redundant system

자기 테스트 (self test) 동안 마스터 CPU는 스탠바이 CPU의 메모리를 비교하여 상이하면 단독 모드로 전환되고 이때의 에러 발견 과정은 다음과 같다.

① 자기 테스트 상태에서 이중화 CPU (마스터와 스탠바이)의 메모리를 비교하여 에러가 발견되면
② 시스템을 이중화 시스템 모드에서 단독 모드

3.1 PLC 스탠바이-마스터 전환 운전 및 연속 운전에 관한 방법 및 결과는 다음과 같다.

1). 고장 발생 전 (정상적인 운전 상태)

OB1 실행 (마스터)	OB1 실행 (스탠바이)
:T QB z	:T QB z
:L DW x	:L DW x
:KB 1	:KB 1

이 경우 마스터로 운전되며 스탠바이와 동기화 운전을 한다.

2) 고장 발생 (마스터에서 고장 발생)

마스터	스탠바이
:T DW x	:T DW x
:AW	:AW
:마스터에서 고장 발생	:L PW y
	:T FW
	:A F x.y
	:스탠바이로 운전

스탠바이 상태에서 고장이 발생하여 마스터로 전환되는 경우도 동일한 결과를 얻었다. 이 경우에 마스터가 스탠바이 상태로 스캔하고 있는 경우에만 가능하였고 마스터와 스탠바이 시스템이 동시에 고장이 발생한 경우는 시스템이 정지되는 것을 확인하였다.

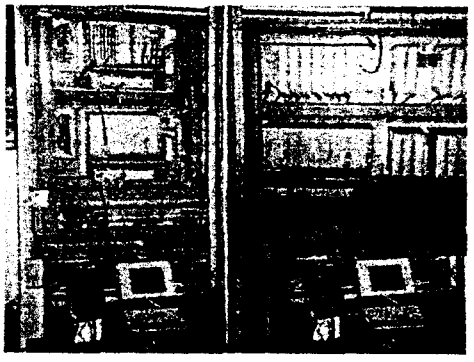

그림7. 실험중인 PLC 고장에 대한 이중화 시스템
Fig7. Testing of reduandancy system for fault-tolerant of PLC

3.3 실제 PLC 고장 허용 이중화 제어 시스템에 적용 결과

시뮬레이션 결과를 확인하여 PLC 고장에 대하여 연속 운전 상태를 확인한 후 실제 고장 허용 제어가 필요한 소성로(燒成爐.kiln)의 제어에 적용하여 PLC 고장에 대한 이중화 시스템을 구성하여 실시간 제어 시에 발생되는 고장에 대하여 연속 운전이 가능한 것을 검증하였다. 시스템의 구성은 그림2와 같이 하였으며 유저(user) 프로그램은 OB, PB, FB, DB을 작성하여 적용하였으며 시스템의 운전 및 안정적인 운전을 확인하였다.

4. 결론

PLC 제어 시스템의 고 신뢰화를 위하여 고장 개소의 영향을 다른 개소에 미치지 않고 시스템의 운전을 연속시키는가 즉 고장허용이 중요하다. 본 논문에서는 연속 운전이란 관점에서 고장허용을 고려한 이중화 시스템에 대하여 설명하였다. 이 고장허용에 대한 이중화 시스템은 고장을 조기에 발견하고 고장으로 인한 손실 및 사고를 미연에 방지함으로써 시스템의 신뢰도를 증가시킨다. PLC 제어 시스템의 고장 시 고장 부분을 시스템의 정지 없이 복구할 수 있는 구조가 가능하고 본 논문에서는 마스터와 스탠바이 그리고 각종 모듈의 이중화를 적용하고 시스템 프로그램, 유저 프로그램을 작성하여 시뮬레이션을 실시한 결과 고장허용 제어가 실현되었고 이 결과를 바탕으로 실제 고장허용 제어가 필요한 소성로(燒成爐.kiln)설비에 적용하여 PLC 제어 시스템의 고장 시에 연속 운전이 가능한 것을 확인하였다. 이러한 고장허용에 연속 운전 방법은 제어 시스템의 고장 시 많은 생산량의 손실을 가져오는 경우와 고장 시에 따른 적은 생산 손실이라도 주위의 공정에 막대한 영향을 미치는 경우 또는 복구 및 손실 비용이 많은 경우 그리고 안 전상 중요한 설비에는 고장허용에 대한 이중화 시스템을 적용하면 효과적일 것이다.

참 고 문 헌

[1] SIEMENS SIMATIC "S5-155 programmable controller' manual C79000-B8576 -C197-05.

[2] SIEMENS Hans Berger "Automating with the SIMATIC S5-115U" 1989.

[3]SIEMENS SIMATIC "S7-400H programmable controllers fault-tolerant systems," manual C7900-G8276-C508-01

[4] SIMATIC S5 "programmable controller S5-155U" manual 6ES5998-00M22 Release 04.

[5] 이상효, 임화영 "S5-115U 프로그래머블 콘트롤러 사용 설명서" 광운 대학교 출판부.