

필드버스 인터페이스를 위한 결합내성형 마이크로컨트롤러

김병진, 이인환
(한양대학교 전자전기공학부)

A Fault-Tolerant Microcontroller for Fieldbus Interface

Byungjin Kim, Inhwan Lee
(Division of Electrical and Computer Engineering, Hanyang University)

요약 - 본 논문은 필드버스 인터페이스를 위한 이중구조의 결합내성형 마이크로컨트롤러 구조를 제시하고, 테스트 환경을 구축하여 고장허용 기능을 검증한다. 이중구조의 결합내성형 마이크로컨트롤러는 두 개의 프로세서 모듈의 출력을 비교하여 고장을 발견하고, 고장을 발견한 경우 버스 출력을 차단함으로써 전체 시스템의 오동작을 방지한다. 일단 고장을 발견하면 자체 진단을 통해 고장 상태를 판단하여, 영구적인 고장일 경우 정지하고 일시적인 고장일 경우에는 재시작을 통해 정상동작으로 복구함으로써, 고장정지 및 일시적인 고장으로부터의 회복기능을 제공한다. 이중구조의 결합내성형 마이크로컨트롤러에 필드버스 인터페이스 기능을 추가하여 자체적인 응용 노드로서의 기능을 수행할 수 있도록 한다. 그리고 이러한 노드를 MC68360프로세서를 이용하여 구현하고, 인위적인 고장주입을 통하여 그 기능을 검증한다.

스트 환경을 구축한다. 일반노드와 함께 필드버스로 연결된 테스트 환경에서 네트워크 응용 노드로서의 성능과 고장허용 기능을 검증한다.

2. 이중구조의 결합내성형 마이크로컨트롤러

본 절에서는 결합내성을 갖지 않은 두 개의 마이크로프로세서를 이용하여 결합내성형 마이크로컨트롤러를 실현하기 위한 이중구조를 소개하고, 비교기 출력이 정상상태로 고정되는 고장을 발견하기 위한 방법을 제시한다.

제안된 이중 마이크로컨트롤러는 그림1과 같이 두 개의 프로세서 모듈, 자체적으로 클럭의 고장유무를 판단 가능한 공통의 자체진단형 클럭, 두 프로세서 모듈의 외부 출력을 비교하여 고장을 발견하는 비교기회로, 두 프로세서 모듈의 동작시점을 일치시키는 동기화회로 및 고장 발견 시 외부 출력을 차단하는 스위치회로로 구성된다.

1. 서 론

산업용 분산 제어시스템, 자동화 시스템 등의 개방형 제어시스템을 구축하기 위해서는 각 필드기기에서 생산되는 정보들을 적절한 형태로 가공하여 적시에 필요한 공정으로 제공하여 줄 수 있는 표준화된 필드기기의 도입이 필요하다. 필드버스는 이러한 필드기기들이 정보를 교환하고 공유하기 위한 기반기술이다. 필드버스 기반시스템의 사용이 증가할수록 이러한 시스템에 대한 신뢰도 요구조건 또한 증가하고 있다. 본 논문에서는 필드버스 기반시스템의 신뢰도와 안정성을 향상시키기 위한 방법으로서 노드의 오동작을 방지하기 위한 이중구조의 결합내성형 마이크로컨트롤러 구조를 제시하고 검증한다.

전체 시스템의 오동작을 방지하기 위해서 노드는 고장이 발생할 경우 즉시 스스로의 동작을 정지시켜 외부로 잘못된 결과를 제공하지 않는 기능 즉, 고장정지 기능을 가져야 한다. 또한 일시적인 고장일 경우에는 고장진단을 통하여 회복할 수 있어야 한다. 본 논문에서는 이중 마이크로컨트롤러 구조를 채택하여 영구적인 고장일 경우 정지하는 고장정지의 기능 및 일시적인 고장으로부터의 회복기능을 통한 노드의 오동작을 방지한다.

이중구조의 결합내성형 마이크로컨트롤러는 두 개의 프로세서 모듈의 출력을 비교하여 고장을 발견하고, 고장을 발견한 경우 즉시 버스 인터페이스를 차단함으로써 전체 시스템의 오동작을 방지한다. 일단 고장을 발견하면 자체진단을 통해 고장 상태를 판단하여, 영구적인 고장일 경우에는 정지하고 일시적인 고장일 경우에는 재시작을 통해 정상동작으로 복구함으로써, 고장정지 및 일시적인 고장으로부터의 회복기능을 제공한다(1).

본 논문에서는 두 프로세서 모듈의 출력을 비교하는 비교기 출력이 정상상태로 고정되는 고장을 발견할 수 있는 방법을 제안하고, 하나의 클럭이 고장이 발생하더라도 마스킹 되어 프로세서모듈의 연속 동작을 보장하는 고장허용형 클럭을 설계한다. 이러한 이중구조의 마이크로컨트롤러에 필드버스 인터페이스 기능을 추가하여 테

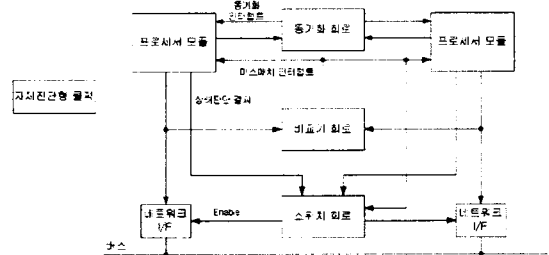


그림 1 이중 마이크로컨트롤러 구조

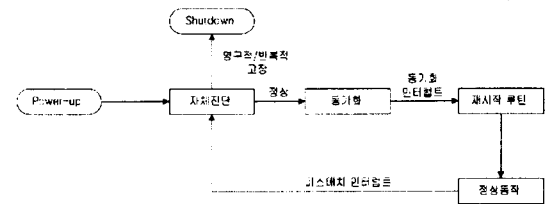


그림 2 이중구조의 동작

이중구조의 동작은 그림2와 같이 자체진단을 수행하여 고장유무를 판단하고 고장이 없을 경우에는 공통 자체진단형 클럭과 동기화회로를 사용하여 두 프로세서 모듈의 동작 시점을 일치시키는 동기화 과정을 수행한다. 동기화를 거친 두 프로세서 모듈은 클럭 단위로 정확하게 일치되어 락스텝으로 동작하게 된다. 이후 정상동작

시 한 모듈에 고장이 발생하여 두 프로세서 모듈의 동작 상태가 달라지면, 이 고장은 프로세서 모듈이 외부 출력을 수행할 때 비교기 회로에서 발견된다. 고장이 발견되면 비교기는 고장신호를 스위치 회로에 전달하여 외부 출력이 즉시 차단되도록 한다. 또한 동시에 프로세서 모듈에 미스매치 인터럽트를 발생시켜 두 프로세서 모듈이 자체진단을 수행하도록 한다. 이중구조는 자체진단의 결과 영구적인 고장이 발견되면 정지함으로써 고장정지 특성을 갖는다. 그리고 두 프로세서 모듈이 정상이라고 판단되면 동기화를 통해 동작 시점을 일치시키고, 재시작 과정을 통하여 스위치 회로를 통한 프로세서 모듈의 외부로의 출력을 다시 허용함으로써 일시적인 고장으로부터는 회복하여 정상동작을 수행한다. 자체진단 시에 발견되지 않는 고장은 이후 정상동작으로 복귀 시 또다시 비교기에서 고장신호가 발생하는 원인이 된다. 이 경우 자체진단과 재시작 과정을 반복하는 현상이 발생한다. 반복적인 자체진단 수행 현상이 있을 경우 이를 영구적인 고장으로 판단하여 고장정지를 수행한다.

두 프로세서 모듈이 모두 정상 동작하는 경우 비교기의 출력은 항상 정상 상태 즉 1의 값을 갖게 된다. 따라서 제안된 이중구조에서는 프로세서 모듈의 고장으로 인해 비교기에서 고장신호가 발생하지 않는 한, 비교기 출력이 정상 상태로 고정되는 고장은 발견되지 않게 된다. 또한 프로세서 모듈에 고장이 발생할 확률이 그리 높지 않기 때문에, 하나의 비교기의 출력이 정상상태로 고정된 이후에 계속하여 두 프로세서 모듈이 정상으로 동작할 수 있고, 이 경우 이중구조는 영구적인 고장이 발생한 상태로 계속하여 동작을 하게 된다. 그리고 만약 하나의 비교기 출력이 정상 상태로 고정된 이후 나머지 비교기에서도 동일한 고장이 발생하게 되면, 프로세서 모듈의 출력이 실제로 틀려지더라도 두 비교기에서 고장신호가 발생하지 않게 되어 잘못된 결과가 외부로 전달되는 문제점이 발생할 수 있다. 이러한 고장형태는 단일 고장이 아니라 이중 고장으로써, 일반적인 단일 고장허용 시스템 설계 시에는 고려하지 않는 사항이다.

하지만 본 논문에서는 출력이 정상상태로 고정되어 발견되지 않는 형태의 이중 고장에 대해서도 이중구조가 고장정지를 수행할 수 있도록 설계한다.

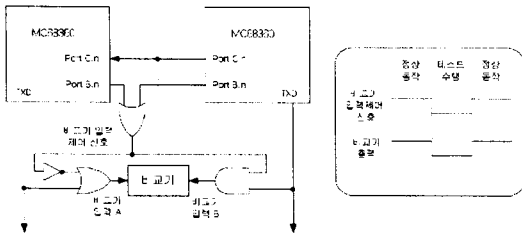


그림 3 비교기 출력의 정상상태로의 고정에 대한 제어

비교기 출력의 정상상태로의 고정을 발견하기 위해서는 정상 동작 중에 인위적으로 비교기의 출력을 고장상태로 바꾸고, 이를 검사함으로써 비교기의 출력이 정상상태로 고정되었는가를 판단하는 과정이 필요하다. 본 논문에서는 그림 3과 같이 여분의 하드웨어를 추가하여 비교기 출력의 정상상태로의 고정을 검사한다. 테스트를 수행하지 않을 때 프로세서 모듈은 포트 B.n으로 1을 출력하고, 이 경우 비교기에는 각 프로세서 모듈의 출력이 그대로 전달되게 된다. 매번 출력이 끝난 후 테스트를 수행할 때 프로세서 모듈은 인터럽트를 마스킹 한 후 포트 B.n으로 0을 출력한다. 두 프로세서 모두 0을 출력하게 되면, 비교기 입력 제어신호가 0이 되어 비교기 입력 전단의 OR 게이트로는 1이, AND 게이트로는 0

이 각각 비교기에 입력되어 비교기의 출력은 고장상태로 바뀌게 된다. 따라서 이때 포트 C.n의 값을 읽어봄으로써, 비교기 출력의 정상상태로의 고정 여부를 검사한다. 검사가 끝난 후 프로세서 모듈은 인터럽트 대기 비트를 지우고, 포트 B.n으로 1을 출력하고 미스매치 인터럽트 인에이블 시킨 후 정상동작을 수행한다.

비교기 출력의 정상상태로의 고정을 검사하는 추가적인 하드웨어는 그 자체에서 고장이 발생할 수 있다. 하지만 비교기 검사를 위한 하드웨어의 고장은 결국 정상 동작과 테스트 과정 시의 비교기 입력에 영향을 주게 되어, 비교기에서 고장이 발생한 경우와 동일한 현상으로 발견이 되고, 따라서 비교기 검사를 위한 하드웨어의 고장에 대해서도 이중구조가 고장허용 기능을 갖는다.

3. 클럭의 고장허용

락스텝으로 동작하는 이중 마이크로콘트롤러의 공통클럭에 고장이 발생하게 되면 전체 시스템이 오동작을 할 수 있다. 따라서 클럭은 그 자체가 고장허용 기능을 가져야 한다.

제안된 이중구조의 고장허용 클럭은 자체점검 능력을 갖는 클럭을 다수 사용하여 사용 중인 클럭에 고장이 발생한 경우 다른 정상 클럭으로 전환하는 방법을 이용하여 설계하였다[7]. 그러나 이러한 방법에서는 클럭에 고장이 발생하여 정상클럭으로 전환할 때 프로세서를 연속적으로 동작시키기 어려운 단점이 있다.

따라서 본 논문에서는 자체진단 기능을 갖지 않는 클럭을 다수 사용하고 이들의 동작을 비교하여 전체적으로 하나의 고장허용형 클럭을 사용함으로써 하나의 클럭에 고장이 발생하더라도 이를 마스킹 하여 클럭 고장 시 프로세서를 연속적으로 동작시킬 수 있도록 설계한다.

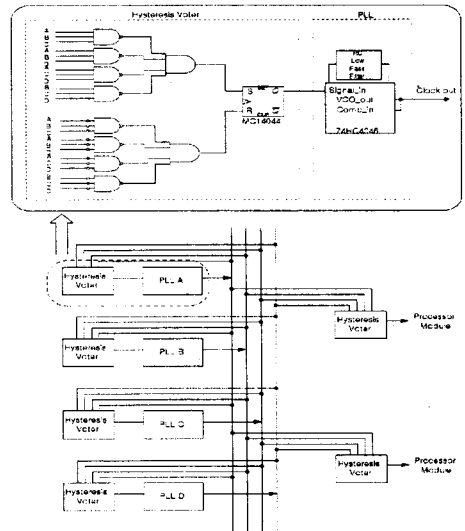


그림 4 고장허용형 클럭

일반적인 TMR (Triple Modular Redundancy) 구조를 클럭의 설계에 적용할 경우 각 클럭 모듈의 출력은 기본적으로 동기가 되어 있지 않아 다수결 보팅이 의미를 상실하기 때문에 원하는 고장허용 기능을 얻을 수 없고, 하나의 클럭 고장을 마스킹 할 수 있는 고장허용형 클럭은 네 개의 오실레이터와 이들의 출력을 처리할 수 있는 소위 히스터리시스 보터를 다수 사용하여 실현할 수 있다[8].

본 논문의 고장허용형 클럭은 그림 4와 같은 구조를 가진다. 이 구조는 4개의 PLL(74HC4046과 RC 저역 통과 필터)과 4개의 히스테리시스 보터로 구성된다. PLL은 주파수 발전을 위한 VCO(Voltage Controlled Oscillator), 위상 검출기, RC 저역통과 필터로 구성된다. 각 히스테리시스 보터는 4개의 PLL의 출력을 바탕으로 공통 클럭 신호를 만든다. 각 PLL은 위상 검출기를 통해 히스테리시스 보터 출력과 자체 VCO 출력간의 위상 차를 검출하고, RC 저역통과 필터를 사용하여 VCO 출력 주파수를 조정하는 페이즈 락킹(phase locking)을 수행함으로써 4개의 PLL 출력간의 주파수와 위상을 정확히 일치시킨다. 이를 통해 정상 시에 모든 PLL은 동일한 주파수와 위상으로 동작을 하게 되고, 만약 하나의 PLL에서 고장이 발생하더라도 히스테리시스 보터에 의해 고장이 마스킹 되어 나머지 3개의 정상 오실레이터는 일치된 주파수와 위상으로 동작을 계속 수행한다. 또한 각 프로세서 모듈은 4개의 PLL 출력을 보팅하여 클럭으로 사용한다.

4. 필드버스 인터페이스 및 고장허용 기능 검증

이중구조 마이크로컨트롤러는 모토몰라의 MC68360 프로세서와 범용 로직 IC를 이용하여 구현하였다. 구현된 마이크로컨트롤러는 그림5에서와 같이 각각 두개씩의 프로세서 모듈, 동기화회로, 스위치회로 그리고 비교회로로 구성된다.

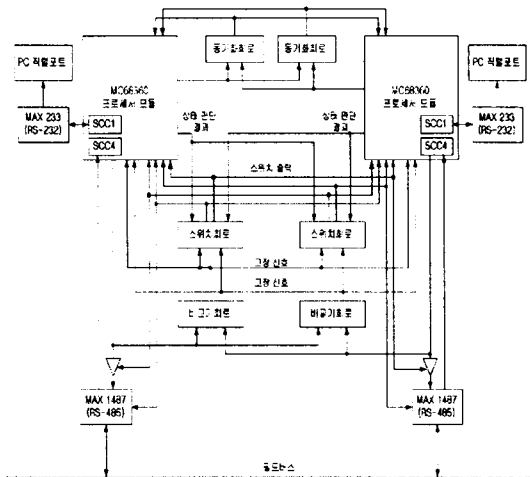


그림 5 필드버스 인터페이스를 위한 이중구조 구현

필드버스 인터페이스를 위해서는 Profibus의 물리계층과 데이터링크계층을 구현하였다(4). 그림5의 짙은 색 부분은 필드버스 인터페이스를 위한 부분으로서 MC68360의 SCC(Serial Communication Controller)에서 제공하는 직렬통신기능과 필드버스와 연결되는 RS-485 통신부, 네트워크 모니터링을 위한 RS-232 통신부를 이용하여 구성하였다.

정상동작시 이중구조 노드의 두 프로세서 모듈은 같은 입력을 동시에 받아들여야만 일치된 상태로 락스텝 동작이 가능하다. 따라서 필드버스를 통한 입력은 각각의 RS-485 트랜시버를 통하여 이루어진다. 그러나 버스출력의 경우에는 RS-485 트랜시버의 DE(Driver Output Enable)신호와 라인버퍼를 제어하여 출력이 허용된 둘 중 하나의 트랜시버 출력만을 허용한다.

필드버스 인터페이스 기능을 갖는 이중구조 노드의 네

트위크 응용 노드로서의 기능과 고장허용 기능을 검증하기 위하여 고장허용 기능이 없는 일반노드와 함께 필드버스로 연결된 테스트 환경을 구축하였다. 필드버스 시스템에서 각 노드는 고유한 주소를 가져야 하므로 이중구조 노드의 주소는 1번으로 일반노드의 주소는 2번으로 각각 할당하였다. 이중구조 노드는 전원 공급 후 자체진단을 수행하여 고장이 발견되지 않을 경우 동기화 과정을 거친다. 동기화를 통하여 이중구조 노드의 두 프로세서 모듈은 락스텝으로 동작하기 시작한다. 2번 주소를 가지는 일반노드와 이중구조 노드는 필드버스 시스템의 초기화 작업을 수행한다. 초기화 작업은 최하위 주소 노드인 2번 노드가 토큰을 생성하여 논리적인 토큰링을 생성하는 것이다. 정상적으로 필드버스 시스템이 초기화되면 토큰을 가진 노드만이 데이터를 전송하며 안정상태를 유지한다. 테스트 환경에서 각 노드는 타이머 인터럽트를 이용하여 주기적으로 메시지를 생성하고 이를 통해 노드들 간에 데이터를 주고받게 한다.

번호	고장주입 위치
1	프로세서 모듈의 데이터 버스 (D0~D4)
2	프로세서 모듈의 직렬출력(TXD)
3	동기화회로의 출력
4	스위치회로의 출력
5	비교회로의 출력

표 1 인위적인 고장주입 위치

이중구조 노드는 실제 필드버스 응용 환경에서 네트워크 노드로서의 기능 및 고장허용 기능을 수행한다. 이러한 기능들은 네트워크 모니터링을 통한 분석과 인위적인 고장주입을 통하여 검증하였다. 네트워크 모니터링 기능은 MC68360 프로세서와 PC의 직렬 통신포트를 연결하여 해당노드의 토큰과 데이터 프레임의 송수신과 프로토콜상의 상태천이를 출력해주도록 구현되었다. 또한 고장허용기능의 검증을 위하여 이중구조 노드의 자체진단과 동기화시 그리고 일시적 고장으로부터의 회복 및 고장정지 시에도 메시지를 출력하는 기능을 추가하였다. 정상동작중 인위적인 고장주입은 표1 에서와 같은 고장주입 위치에 stuck-at-low의 영구적 고장과 10μs 동안 low 신호를 유지하는 일시적 고장을 주입하였다.

```
>>
** -lsanyang University - **
** A = serial-to-parallel Microcontroller
   For -fieldbus Interface - **
>>
F1 : self-checking ...
F2 : self-checking ...
F3 : synchronization ...
F4 : synchronized start
```

```
ST0 :-----Offline-----
          loc addr = 01
ST2 : -A-
          DCG token
          01820C0182
Get Token from (02) to me(01)
ST9 : Check_T_P = 03
          CG_SDI
          0703697316
          SC : IN-STP
          Pass Token = 002
```

```
S'8 : -Check_T_P = 03
          DCG token
          01820C0182
[고장주입시]
FT1 : self-checking ...
FT2 : fault count = 1
FT3 : synchronization ...
FT4 : synchronized start
ST0 :-----Offline-----
          loc addr = 01
```

```
S'8 : -Check_T_P = 03
          DCG token
          01820C0182
ST4 : -T-
ST7 : -PT-
          Pass Token to [T]
[고장주입시]
FT1 : self-checking ...
FT0 : stopped !
```

그림 6 필드버스 기능 및 고장허용 기능 검증

그림6은 이중구조 노드의 필드버스 노드로서의 네트워크 기능및 비교기의 출력에 인위적 고장을 주입하였을 때의 고장허용 기능을 검증한 예이다. 그림의 'FT'로 시작하는 메시지는 이중구조의 고장허용 기능을 만족시키기 위한 동작을 나타내고 그 이외의 메시지는 필드버스 프로토콜에 의한 네트워크 기능 수행을 나타낸다.

①번 출력을 통해 이중구조 노드가 전원공급시에 자체진단과 동기화 과정을 거쳐서 락스텝으로 시작되었음을 확인할 수 있다. ②번 출력은 1번 노드인 이중구조 노드가 2번 노드로부터 토큰을 수신하고 확인한 후에 다시 2번 노드로 토큰을 넘겨주는 것을 출력한 메시지이다. 따라서 이중구조 노드가 필드버스 인터페이스 기능을 수행하고 있음을 확인할 수 있다.

③번과 ④번 출력은 이중구조 노드에 인위적인 고장을 주입했을 때의 동작을 나타낸다. ③번의 경우에는 비교기 출력이 일시적으로 0이 되도록 인위적인 고장주입을 했을 경우를 나타낸다. 고장은 토큰수신중에 주입이 되었다(DCG token 0182DC01...). 이중구조 노드는 즉시 미스매치 인터럽트를 발생시켜 RS-485 트랜시버의 출력을 차단하고 자체진단을 수행한다(FT1 : self-checking ...). 자체진단 수행 후 내부에 고장이 발견되지 않아 일시적인 결함으로 판단하고 고장횟수를 기록한다(FT2 : fault count = 1). 그리고 다시 재시작 하여 일시적인 결함으로부터 회복한다(FT4 : synchronized start !).

④번의 경우에는 정상동작중에 비교기의 출력이 stuck-at-low가 되도록 인위적인 고장을 주입했을 경우를 나타낸다. 고장은 이중구조 노드가 2번 노드에게 토큰을 보내려고 하는 도중에 주입되었다(Pass Token to...) 즉시 미스매치 인터럽트를 발생시키고, RS-485 트랜시버의 출력을 차단한다. 그 후 이중구조 노드는 자체진단을 수행하여 비교기의 영구적인 고장으로 판단하고 정지한다(FT0 : stopped !). 이를 통해 영구적인 고장으로부터 정지하는 고장정지 특성을 검증하였다.

표1에서 비교기출력 이외의 나머지 고장주입위치에도 인위적인 고장의 주입을 통하여 일시적인 고장일 경우 이중구조 노드는 자체진단과 재시작 과정을 통한 고장회복의 기능과, 영구적인 고장일 경우에는 버스출력을 차단하고 정지하는 고장정지 특성이 만족함을 검증하였다.

5. 결 론

본 논문에서는 필드버스 기반시스템의 신뢰도와 안정성을 향상시키기 위한 방법으로 노드의 오동작을 방지하기 위한 이중구조의 결함내성형 마이크로컨트롤러 구조를 제시하고 필드버스를 이용한 테스트 환경에서 응용노드의 기능과 고장허용 기능을 검증하였다.

기존에 제안된 이중구조의 결함내성형 마이크로컨트롤러는 두 프로세서 모듈의 동작을 비교하여 고장을 발견하고, 고장발견 시 즉시 필드버스 인터페이스를 차단함으로써 오동작을 방지한다. 고장 발견 시에는 자체진단을 통해 상태를 판단하여 영구적인 고장일 경우에는 정지하고, 일시적인 고장일 경우에는 동기화와 재시작 과정을 거쳐 정상동작으로 복귀함으로써 고장정지 및 일시적 고장으로부터의 회복특성을 갖는다.

본 논문에서는 비교기회로의 출력이 정상상태로 고정되어 발견되지 않는 형태의 고장에 대해서도 발견 할 수 있는 방법을 제안하고, 하나의 클럭에 고장이 발생하더라도 이를 마스킹 하여 클럭고장 시에도 프로세서를 연속적으로 동작시킬 수 있는 공통 고장허용형 클럭을 설계하였다. 이러한 이중구조의 마이크로컨트롤러는 실제 네트워크 응용환경에서의 검증을 위하여 모토롤라의 MC68360 프로세서와 로직 IC를 이용하여 구현하고, 필드버스 인터페이스 기능을 추가하였다.

일반노드와 필드버스로 연결된 테스트 환경에서 네트

워크 모니터링 기능을 이용한 검증을 통하여 이중구조 노드의 기능을 평가하였다. 이중구조 노드는 필드버스를 통한 네트워크 기능을 수행하는 노드로서의 기능과, 정상동작중 인위적인 고장주입을 통하여 응용환경에서의 고장허용 기능이 만족함을 확인하였다.

(참 고 문 헌)

- [1] 백승수, 이인환, "이중구조의 결함내성형 마이크로컨트롤러" 대한전기학회 하계학술대회 논문집 pp. 2859-2862, 1999
- [2] J.-C. Laprie, Dependability: Basic Concepts and Terminology, Springer-Verlag, 1991.
- [3] B. W. Johnson, Design and Analysis of Fault-Tolerant Digital Systems, Addison-Wesley Publishing Company, Inc., 1989.
- [4] 홍승호, 임동진, 이인환 "컴퓨터 Interface를 위한 Intelligent Sensor" 한국과학재단 특장기초 연구과제 제2차 중간보고서, pp. 12-24, 1999
- [5] W. N. Toy, "Fault-Tolerant Design of Local ESS Processors," Proceedings of the IEEE, Vol. 66, No. 10, pp. 1126-1145, Oct. 1978.
- [6] MC68360 Quad Integrated Communications Controller User's Manual, Motorola, 1993.
- [7] A. M. Usas, "A Totally Self-Checking Checker Design for the Detection of Errors in Periodic Signals," IEEE Transaction on Computers, Vol. c-24, No. 5, pp. 483-488, May 1975.
- [8] W. M. Daly, A. L. Hopkins, J. F. McKenna "A Fault-Tolerant Digital Clocking System" IEEE Proceedings of FTCS-25, Volume III, pp. 17-22, 1973