2002년도 대한전기학회 하계학술대회 논문집 2002.7.10-12

원전용 이더넷 기반 실시간 제어 통신망을 위한 결함 허용 방법

문병길, 김형석, 권욱현
서울대학교 전기컴퓨터공학부

이성우, 김석곤, 송성일
한국 전력 연구원

Fault-Tolerant Methods of Ethernet-based Real-Time Control Network for Nuclear Power Plants

Byung-Kil Moon, Hyung Seok Kim, Wook Hyun Kwon
School of Electrical Engineering, Seoul National University

Sung Woo Lee, Seok Gon Kim, Seong Il Song
Korea Electric Power Research Institute

Abstract - 본 논문에서는 원자력 발전소용 이더넷 기반 링형 실시간 제어 통신망인 ERCNet(Ethernet-based Real-Time Control Network)에서 고신뢰성을 유지하기 위한 결함 허용 방법들을 제시한다. 임의의 노드의 프로그램 동작에 이상(fault)이 발생하였을 경우, 와치독(Watchdog) 타이머로 탐지하여 링을 자동 복구하고, 그 노드가 다시 회복될 경우의 노드 추가 메커니즘을 제안한다. 이 메커니즘은 한 노드가 전체 네트워크에서 제외되거나 추가될지라도 네트워크가 운용성(operability)을 유지할 수 있도록 한다. 두 번째로, 한 채널 또는 양 채널 에러 발생시 이 에러를 대처하기 위한 채널 이중화 방식과 시스템 이중화 방식에 대해 제안한다. 마지막으로 통신망의 임의의 위치에서 이상이 발생했을 경우, 그 발생 위치를 파악할 수 있는 메커니즘을 제안한다.

1. 서 론

원자력 발전소는 안전성을 최우선으로 하는 복잡한 대규모 시스템으로써 주제어 실에는 4000여 개의 경보 및 감시장치들이 설치 되어 있다. 발전소 운전원은 방대한 양의 정보들을 처리하면서 발전소를 제어하며 최적정격 출력 운전을 한다. 그러나 발전소가 과도현상, 운전 정지, 또는 비상상태로 되면, 사건 초기에 약 500여개 이상의 경보가 발생되고, 많은 운전변수들이 동시에 변하여 운전원에게 부담을 준다[1]. 원자력 발전소에 사용되기 위한 시스템은 무엇보다도 신뢰성이 중요하다. 특히, 여기에 사용되는 시스템 중, 통신망 시스템은 정확한 데이터의 전달과 부시스템들에 대한 결함에 대한 대처가 필수적이다. 통신망 시스템 중에서 결함을 많이 내포하고 있는 부분으로서 하드웨어에는 전송 매체와 네트워크 인터페이스 카드(Network Interface Card, NIC)가 있고, 소프트웨어에는 통신을 담당하고 있는 데이터 전송 및 수신 모듈이라고 할 수 있다. 전송 매체는 환경에 노출되어 있기 때문에 노이즈가 타기 쉬울 뿐만 아니라 끊어질 우려가 있고, NIC은 일반적으로 중앙처리장치가 있는 CPU 보드와 착탈식으로 이루어 있기 때문에 접촉 불량이 되거나 시간이 경과하면 마모되어서 이 부분으로도 노이즈가 타서 잘못된 통신 결과를 초래할 수 있다. 뿐만 아니라, 통신 소프트웨어는 메모리나 레지스터의 순간적인 결함에 의해 작동이 중지되거나 예상치 못한 행동을 할 수 있다. 그래서, 이러한 결함 요소들을 예측하여 대처 방안을 모색하는 것은 원자력 발전소용의 시스템에 있어서 필수 불가결하다.

현재까지 통신망에 대한 여러 종류의 결함 허용에 대한 연구가 있었다[4]-[8]. 그 중에 [6], [7], [8]에서는 물리 계층의 이중화에 대한 연구가 있었다.

본 논문에서는 원자력 발전소용으로 새롭게 설계된, 광매체를 사용하며 전이중 고속 이더넷(Full-Duplex Fast Ethernet)을 기본으로 한 토큰 링형(Ring Topology) 실시간 분산 제어 시스템인 ERCNet을 위한 결함 허용 방법들을 제안한다. 먼저, 본론에서, ERCNet의 구조와 동작 방법을 간략히 설명한 후, 임의의 노드의 프로그램 진행에 결함(fault)이 발생하였을 경우에 와치독(Watchdog) 타이머로 탐지하여 링을 자동 복구하고, 그 노드가 다시 회복될 경우의 노드 추가 메커니즘을 제시한다. 그리고, 한 채널 또는 양 채널에 에러가 발생할 경우, 이를 대처하기 위한 채널 이중화 방식과 시스템 이중화 방식을 제안하고, 통신망의 임의의 위치에서 이상(fault)이 발생했을 경우 그 발생 위치를 파악할 수 있는 메커니즘을 제안한다. 그리고, 결론에서 이 논문의 결과를 맺는다.

2. 본 론

2.1 ERCNet 구조 및 동작

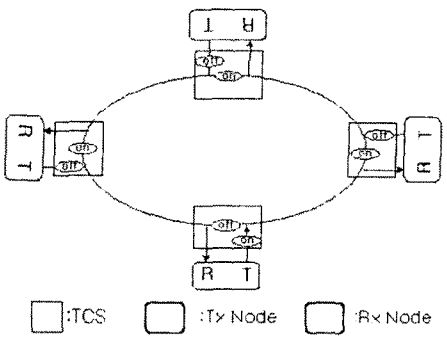

그림1. ERCNet 구조 및 동작

ERCNet은 물리적으로는 링형 구조를 갖고 있지만, 실제 데이터 전송하는 과정에서는 버스형으로 바뀌어진다. 그리고, 이러한 링형에서 버스형으로 변환되는 동작은 TCS(Topology Conversion Switch)라는 NIC에서의 스위칭 동작에 의해 이루어지는데 송신 노드와 수신 노드에서 차이가 있다. 그림1은 송신하는 노드와 수신하는 노드에서의 TCS의 동작 모습을 보여준다. 그림에서 보는 바와 같이 송신 노드에서 전송한 프레임은 수신 노드의 버퍼를 거치지 않고 곧바로 자신에게 돌아오게 된다.

기타 ERCNet의 특징은 아래와 같다[2].

- 데이터 링크 계층에서의 전이중 고속 이더넷 프로토콜 응용한 토큰 링 네트워크
- 브로드캐스팅(Broadcasting)으로 프레임 전송
- 광매체를 이용한 노이즈 억제와 전송 지연 최소화
- 관리 노드(Manager Node, MN)에서 결함 허용 제어
- 이더넷 프레임의 Type필드를 이용한 프레임 구분

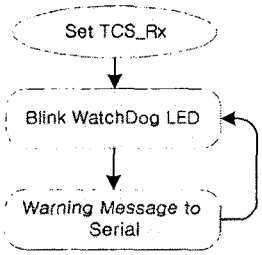

그림2. 와치독 타이머 인터럽트 서비스 루틴

2.2 노드 이상과 회복에 따른 자동 링 복구

통신 프로그램은 주기적으로 와치독 타이머의 값을 초기화 시킨다. 와치독 타이머는 타임 아웃이 되면 인터럽트를 발생시킬 수 있는 특수한 타이머이다[3]. 만약 통신을 하다가 프로그램에 이상이 발생되면, 프로그램은 타이머 값을 초기화시키지 못하므로 타임아웃이 발생하게 되고, 그 노드는 와치독 타이머 인터럽트 서비스 루틴을 실행하게 된다. 그림 2는 이 서비스 루틴에서 실행되는 것을 나타낸 것인데, 우선 TCS를 수신 모드로 만들어서 다른 노드들이 전송하는 프레임이 끊어지지 않도록 한 다음, LED를 깜빡이거나 직렬 포트에 메시지를

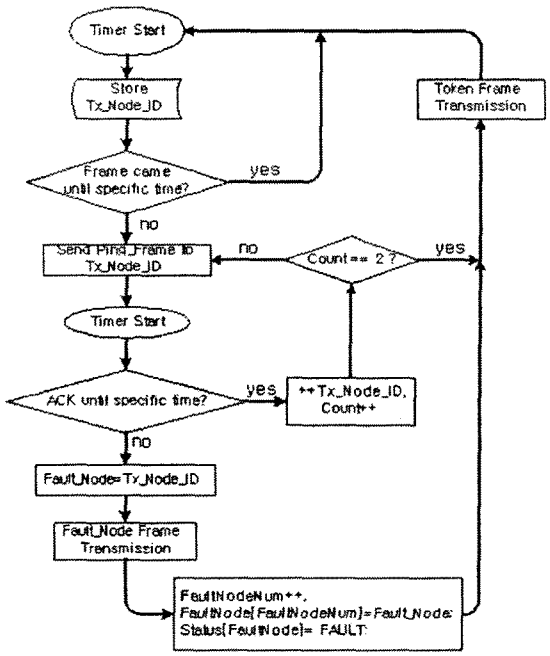

그림3. 관리 노드의 처리 루틴

계속 보내서 관리자에게 노드의 상태를 알리게 된다. 노드에 이상이 생기면 토큰이 그 노드에 전달될지라도 아무런 프레임이 전송되지 않는다. MN은 이 사실을 타이머를 이용해서 알아차리고, 그 노드가 제대로 작동하는지 알아낸 후, 그 노드의 이상을 알리는 제어 프레임(Fault_Node Frame)을 브로드캐스팅해서 모든 노드들로 하여금 이 사실을 알린다. 그림 3은 관리 노드에서 행해지는 이상 노드 파악과 그에 대한 처리 루틴을 나타낸 것이다. 이상 노드 파악은 전송 노드의 번호를 저장하면서 통신의 이상유무를 감시하다가 타임 아웃이 되면, 마지막으로 던진 노드와 그 다음 토큰을 가질 노드

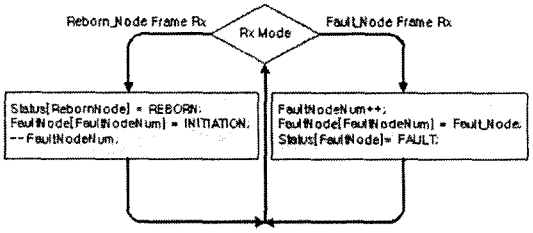

그림4. 일반 노드의 처리 루틴

에게 제어 프레임(Ping Frame)을 전송해서 응답의 유무를 통해서 알아내게 된다.

관리 노드로부터 이 사실을 알게 된 일반 노드(General Node, GN)들은 그림 4와 같이 이상 노드의 정보를 FaultNodeNum, FaultNode, Status 변수들을 이용해서 기억하고, 이후에는 기록된 이상노드에게는 토큰을 던지지 않는다.

그리고, 만약에 그 노드가 다시 회복되는 경우를 대비해서 MN은 자기에게 토큰이 오면, FultNode변수를 이용해서 이상이 발생했던 노드에게 제어 프레임(Ping Frame)을 던져서 응답의 유무를 파악한다. 만약에 그 노드가 응답하면, 회복되었다고 판단하고, 이 사실을 제어프레임(Reborn_Node Frame)을 이용해서 전체 노드에게 알린다. 이 제어 프레임을 받은 일반 노드들은 그림4의 왼쪽에 있는 과정을 그치면서 노드 정보를 수정하게 된다. 그런 후 Status배열을 탐색해서 자신의 번호보다 큰 것 중에 가장 작은 번호를 가진 노드에게 토큰을 전송하게 된다. 이렇게 해서 노드의 이상에 관계없이 전체 네트워크는 운용성을 가지면서 통신을 하게 된다.

2.3 이중화 메커니즘

ERCNet은 고신뢰성을 얻기 위한 방법으로 이중화 메커니즘을 사용한다. 한 채널의 에러에 대비한 채널 이중화와 양 채널 에러에 대비한 시스템 이중화가 바로 그것이다.

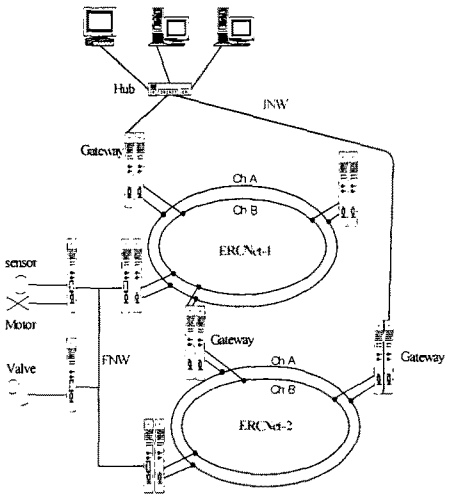

그림5. 이중화 구조

그림5는 이러한 이중화의 모습을 보여주고 있는데, Ch A와 Ch B는 채널 이중화를 나타내었고, ERCNet-1과 ERCNet-2가 시스템 이중화를 나타낸 것이다.

FNW(Field NetWork)는 필드 통신망으로서 원자력 발전소의 실제 감시될 데이터가 있으며, 이 데이터는 ERCNet으로 올려 보내진다. INW(Information NetWork)는 정보통신망으로서 ERCNet을 통해서 올라온 필드 전체의 데이터를 감시하는 운영자들이 사용하기 위한 네트워크이다.

2.3.1 채널 이중화 과정

일반 노드들은 주채널로부터 프레임을 받으면서 정해진 시간 동안 프레임이 오지 않으면, 부채널에서 관리 노드가 던지는 제어 프레임이 오는지 확인한다.

관리 노드는 타이머를 이용해서 항상 주 채널을 감시한다. 만약에 정해진 시간 동안 주채널에 아무런 프레임이 전송되지 않으면 채널 이상(fault)인지 제어프레임(LoopBack Frame)을 이용해서 알아내고, 주채널만 이상이 있고, 부채널은 이상이 없으면, 채널 전환 프레임을 부채널로 브로드캐스팅한다. 부채널로부터 채널 전환 프레임을 받은 일반 노드들은 부채널을 통해서 통신을 유지하게 된다.

2.3.2 시스템 이중화 과정

관리 노드는 부채널에서도 일정시간 동안 채널에 아무런 신호가 오지 않으면(idle), 제어프레임(LoopBack Frame)을 이용해서 양채널을 조사하고, 양 채널에서 모두 에러이면 정보통신망으로 시스템 이중화 메시지를 보내게 된다. 이 메시지를 확인한 정보통신망에 있는 운영자는 ERCNet-2를 통해서 필드의 데이터들을 감시하게 된다.

2.4 채널 결함 위치 파악 메커니즘

MN은 채널 감시 중에 타임아웃이 되면, 채널 A와 B에 제어프레임(Loop_Back Frame)을 전송해서 자신에게 돌아오는지의 유무를 이용해 채널을 모두 검사해서, 채널 B는 정상인데 반해 채널 A에 오류가 있다면 채널 에러 위치 파악 모듈을 실행해서 어느 노드 사이에서 채널 에러가 발생했는지 파악하게 된다.

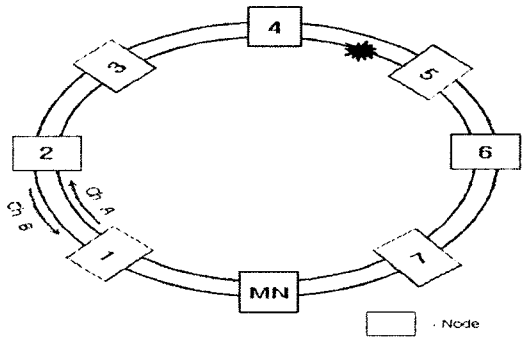

그림6. 채널 에러 위치 파악

채널 에러 위치 파악 과정을 그림6을 보면서 예를 들어 설명한다.

먼저, 채널 A와 채널 B에서의 프레임 전송 방향이 서로 다르게 채널을 설정하고, 관리 노드가 전송하는 제어 프레임(Error_Position Frame)을 수신한 일반 노드들은 ACK를 송신하되 받을 때와는 반대의 채널로 보내게 한다. 그러면, 그림과 같이 채널 A에서의 에러 위치가 노드 4번과 노드 5번 사이라고 생각하자. 관리 노드는 채널 A를 통해서 제어 프레임(Error_Position Frame)을 각 노드들에게 던진다. 이 제어 프레임을 받은 일반 노드들은 채널 B를 통해서 응답을 하게된다. 이런 방식으로 각 노드들에게 폴링(Polling)을 하다보면 4번은 응답을 하는데, 5번은 응답을 하지 못할 것이다. 그러면, 관리 노드는 4번과 5번 사이의 채널에 에러가 발생했다고 판단을 내린 후 직렬 포트를 통해 이 사실을 알리는 메시지를 보내게 된다.

3. 결 론

본 논문에서는 원자력 발전소용으로 개발된 ERCNet에서의 여러 결함 허용 방법들에 대하여 설명하였다.

먼저, 임의의 노드의 프로그램 진행에 결함(fault)이 발생하였을 경우에 와치독(Watchdog) 타이머로 탐지하여 링을 자동 복구하는 메커니즘과 그 이상이 발생한 노드가 다시 회복되는 경우에 따른 통신망의 운용성을 유지하기 위한 관리 노드에서와 일반 노드에서의 구현 알고리즘에 대하여 설명하였다. 그리고, 한 채널 또는 양 채널 에러 발생 시, 이 에러에도 불구하고 통신이 이루어지기 위한 채널 이중화 방식과 시스템 이중화 방식을 전체 하드웨어 구조의 그림과 소프트웨어적인 동작 과정을 보이면서 설명하였으며, 마지막으로 통신망 채널의 임의의 위치에서 이상(fault)이 발생했을 경우, 그 발생 위치를 파악할 수 있는 메커니즘을 채널 이중화를 응용하여 그림을 통해서 관리 노드와 일반 노드 관점에서 구체적으로 설명하였다.

[참 고 문 헌]

[1] R. E. Uhrig, "Potential application of neural networks to the operation of nuclear power plant", Nuclear Safety, vol.32, No.1, pp. 68-78, 1991.

[2] 최재영, 김형석, 권욱현, "실시간 분산 제어 시스템용 고속 전이중 이더넷 기반 통신망의 설계 및 성능 평가", 대한 전기학회 하계 학술대회 논문집, D, 2714 - 2716, 2001

[3] Motorola, "MPC8260 PowerQUICC II User's Manual", Section 4.1.5, 1999.

[4] U. Minoni, G. Sansoni, and N. Scarabottolo, "A fault tolerant microcomputer ring for data acquisition in in dustrial environments", IEEE Trans. on Instrumentation and Measuremnt, vol. 38, no. 1, pp. 32-36, Feb., 1989.

[5] J.-M. Ayache, J.-P. Courtiat and M. Diaz, "REBUS, A Fault-Tolerant Distributed System for Industrial Real-Time Control", IEEE Trans. on Computers, vol. C-31, no. 7, pp. 637-647, July, 1982.

[6] Y. Shiobara, T. Matsudaira, Y. Sashida and M. Chikuma, "Advanced MAP for real-time process control", Proc. of IECON, pp. 883-891, Cambridge, Messachusetts, 5-6, Nov., 1987.

[7] H. Kleines and K. Zwoll, "MAP Mining - A communications system for mining applications", EMUG MAP/TOP EVENTS Conference Proceedings, SYSTEC 92, 1992.

[8] 문홍주, 권욱현, "Mini-MAP 시스템의 결함 허용성을 위한 결함 감지 및 복구 기법", ICASE 논문지, 제 4권, 제 2호, pp. 264-272, April, 1998