MAP 이중화 시스템의 구현

°문 홍주, 박 홍성, 김 원철, 박 정우, 안 상철, 우 원식, 권 욱현
서울대학교 공과대학 제어계측공학과 정보및 시스템 연구실

Implementation of redundant MAP system

°Hongju Moon, Hongsung Park, Woncheol Kim, Jungwoo Park, Sangcheol Ahn, Wonsik Woo, and Wookhyun Kwon
Information Systems Lab., Dept. of Control and Instrumentation Engr. Seoul National University

Abstract

In this paper, the RedMAP, i.e. a redundant Mini-MAP system for high reliability is proposed. Redundancy is implemented for LLC, MAC, and Physical layer of ISL-Mini-MAP. The detection of error of the network, , the broadcasting of the error event, and the network change sequence are three major functions for the dualized Mini-MAP system.

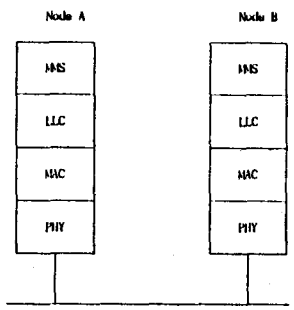
The abnormal operation of the network is mainly detected indirectly with the function of the TBC(token bus controller). The time delay to be required for the change of the networks must be minimized.

With the RedMAP, we can achieve successful transmission only with short additional recovery time.

1. 서론

최근 대형 시스템에 분산 제어를 도입하는 연구및 프로젝트가 여러 곳에서 활발하게 진행되고 있다. 이때 분산 제어 시스템에 필요한 요소 중의 하나가 바로 통신용 네트웍 (network)이다. 이러한 분산 제어 시스템에 쓰이는 네트웍이 갖춰야할 성질로는 고신뢰성, 실시간 특성등이 있다[1]. 특히, 발전소와 같은 시스템의 경우 고장이나 시스템의 정지 등이 발생하는 경우 그 손실이 매우 크므로 시스템에 redundancy를 집어 넣는 것이 필요하다[1]. 네트웍의 경우도 예외는 아니어서 fault-tolerant한 성질이 반드시 필요하다[2]. 본 연구에서는 최근 OSI(open system interconnection) 모델에 기초하여 만들어진 MAP(manufacturing automation protocol)에 redundancy를 넣어 발전소 환경과같이 시스템의 고장에 민감한 경우에도 적용시키기 좋은 이중화 구조의 Mini-MAP인 RedMAP[1]을 개발하였다. MAP은 ISO(international standard organization)에서 규정한 standard network으로 token ring에 기초하여 만들어졌으므로 실시간 제어에 응용하기가 좋고 또한 이종 기기간의 접속에 유리하여 최근 CIM(computer integrated manufacturing), FMS(flexible manufacturing system)등의 분야에서 주목을 받고 있다[3][4][5][6]. 특히 실시간 응답 특성을 좋게 하기위해서 7 계층 구조에서 최상위 계층인 하위의 2계층으로 이루어진 Mini-MAP이 쓰이고 있다.

본연구에서는 대상 시스템을 화력 발전소의 분산 제어 시스템으로 하였으므로 이 Mini-MAP을 대상으로 Redundancy를 넣었다. Mini-MAP의 경우 하위의 2개 계층(Data Link Layer, Physical Layer)은 다시 LLC(Logical Link Layer), MAC(Media Access Layer), 그리고, Physical 계층으로 나누어져서 최상위 계층인 Application 계층와 함께 그림 1과 같이 Mini-MAP을 이룬다[4][5][6]. 또한, 실제 연구의 대상이 되는 Mini-MAP system은 SNU-ISL(Seoul National University - Information Systems Laboratory)에서 개발된 것으로 하였다. ISL Mini-MAP의 경우 그림 1에서 MMS는 host computer에 올라가는 프로그램의 형태로 되어 있고, 그 아래의 나머지 계층들은 slave board에 올라가는 형태로 되어 있다[7][8][9]. 본 연구에서는 LLC 이하 계층을 이중화 하여 한쪽을 주 네트웍(main-network)으로 사용하고 다른 하나를 보조 네트웍(sub-network)으로



• Application layer: MMS
• Data link layer : LLC(class 3)
MAC (token bus)
• Physical layer: Modem(5 Mbps token bus)
Media(75ohm coaxial cable)

주) PHY: physical layer
MAC: media access control
LLC: logical link control
MMS: manufacturing message specification

그림 1

1) 본 연구에서 개발된 Redundant MAP system을 지칭한다.

사용한다. 보통때에 두개의 네트웍은 계속 자신을 감시하고, 주 네트웍(main-network)에 이상이 감지되는 경우 보조 네트웍(sub-network)을 통해 이상 상태를 네트웍상의 모든 station에 알려주고 보조 네트웍(sub-network)으로 전환하도록 하여 한쪽의 네트웍에 이상이 있는 경우에도 전송이 가능하도록 하였다.

2. redundant MAP 의 구현 원칙

본연구에서는 NIU[2](network interface unit)를 2개로 하여 redundancy를 주도록 하고 있다. 즉, 완전히 같은 기능을 하도록 구성된 2 개의 network으로 구성되어 한 쪽의 network에 이상이 있을 때는 이 이상 유무를 감지하여 다른 쪽 network으로 전환 시키도록 되어 있다. 이때 기본적으로 필요한 기능들을 나열해 보면 다음과 같다.

① 이상 상태를 (정확하게) 감지할 수 있어야 한다.
② 가능하면 빠르게 이상 상태를 감지해 낼 수 있어야 한다. 그래야만 가능한 한 통신 data의 손실을 줄일 수 있고 또한 잘못 된 data가 전송되어 system의 동작에 영향을 주는 것을 막을 수 있다.
③ 어느 한 station에서 감지된 이상 상태는 가능하면 빠른 시간내에 모든 station이 알수 있어야 한다.
④ NIU의 변환 즉, network의 변환이 가능해야 한다.
⑤ network의 이상에 의해 잘못 전송된 정보나 손실된 정보에 대한 적절한 처리가 가능해야한다. 이를 위해 이상상태의 발생시점의 추정이나 이상 상태의 발생 시점으로부터 통신망의 변환까지 진행된 일들을 알 필요가 있을 수도 있다.
⑥ network이 전환될때 모든 station들의 sync가 보장되어야 한다. 즉, 모든 station들은 동시에 이상상태를 감지하고 동시에 network의 전환을 수행하도록 되어야 한다. 혹은, network이 전환되는 동안에 진행된 일들에 대한 적절한 처리를 필요로 한다. 만약 그렇지 않으면 network이 변환되는 동안 보낸 data들의, 영구한 손실이나 엉뚱한 정보를 받게되는 경우를 갖게 된다.
⑦ 이상 상태 발생으로 network이 변환된 후 이상상태가 발생된 network의 이상 발생 원인을 찾아내어 가능한 빠른 시간에 복구를 시켜 다시 원래대로 회복시켜 줄 수 있어야 한다.

3. error의 구분 및 종류

error들의 종류를 각 계층별로 나누어 보면 다음과 같다.

①. media의 이상 - cable의 단락, impedance의 변화, noise의 개입
②. modem의 이상 - modem receiver 또는 transmitter의 고장[10]
③. TBC(token bus controller)의 고장 - data 전송이나 수신 기능의 마비, modem interface의 고장, ring management 기능의 마비, cpu system interface 기능의 마비[11]
④. LLC기능의 마비 - CPU system의 마비, 혹은 software 이상
⑤. host interface 기능의 이상 및 MMS에서 보았을때, 전송의 실패

2) LLC, MAC, PHY가 포함되어 있는 ISL Mini-MAP board

4. NIU 전환 방식

양쪽 NIU에서 수신하고 한쪽 NIU만을 통해서 전송하는 방법을 쓴다. 이경우 error없이 동작하는 경우에는 네트웍상의 모든 station에서 동일한 한 네트웍상의 NIU를 통해서 전송하기 때문에 정상상태인 한쪽의 NIU에서만 수신할 data가 올라오기 때문에 하나의 NIU에서 수신하고 하나의 NIU를 통해서 전송하는 경우와 같게 동작한다. 또한 error가 발생하여 네트웍을 전환한 경우에도 역시 한쪽의 보조 네트웍(sub-network)에 물려 있는 NIU를 통해 전송하면 정상상태와 마찬가지로 동작 할 수 있다.

이 경우의 장점은 네트웍의 전환이 이루어지는 동안 네트웍상의 각 station의 전환동작에 대한 synchronization-즉, 그동안 행해 지고 있던 통신 동작들에 대한 적절한 처리 및, 네트웍상의 모든 station이 다른 네트웍으로 전환되는 시점의 확보 -가 자동으로 이루어 진다는 점이다. 다시 설명하면, 양쪽의 통신 창구가 있을 때, 이상이 없는 정상 상태의 창구를 통해 계속적인 송신을 하고 수신측에서는 양쪽을 모두 감시함으로써 어느 한쪽의 창구에 이상이 있어도 수신을 가능하게 할 수 있다. 이경우 송신이 행해지고 있는 동안 네트웍상에 error가 발생하면 이 송신 data는 손실될 수 밖에 없으나 이 error는 LLC와 MMS의 기능에 의해 상위 계층에 송신 실패가 보고되므로 재전송을 통해 data 손실을 막을 수 있다. 이때, MMS가 전송을 끝낸 시점으로 부터 수신측의 응답을 받아 상위 계층에서 재송송을 지시하여 MMS가 재전송을 시작하기 직전까지의 시간보다 네트웍 전환이 빨리 이루어지기만 한다면 error가 있는 경우에도 2회의 재전송만을 통해 정확하고 신뢰성 있는 수행이 가능하다.

양쪽으로 전송하는 방식과의 비교를 해보면, 양쪽으로 전송하기 위해서는 먼저 MMS의 각 service request시마다 양쪽의 NIU를 통해서 transmit를 해주어야 한다. 또한, 양쪽의 NIU에서 data가 올라올 때마다 적절한 처리를 해주어야한다.(수신혹은 receive acknowledge only) 이 경우는 네트웍상에 error가 있을 때도 다른 네트웍쪽의 NIU를 통해 backup된 data를 받아들일 수 있겠지만 이를 위해 추가로 요구되는 overhead가 크다.

data손실의 가능성을 보면 대략 다음과 같이 생각할 수 있다.

$$P_{error} = \sum_{point} \{ P_{err}(point) * P_{pair}(point) * P_{tx} * 2 \}$$

여기서,
P_{error} = 전송중에 error가 발생해서 data에 손실이 생길 확률
$P_{err}(point)$ = 네트웍상의 어느 한 점에서 error가 발생할 확률
$P_{pair}(point)$ = 이 point상의 error에 의해 상호 통신에 장애가 생기는 station의 짝 / 전체 통신 가능 station의 짝
P_{tx} = 어느 한 station에서 송신이 일어날 확률

이때, 네트웍이 bus 형태로 연결되어 있을 때, 평균잡아 error가 이 네트웍의 가운데에서 발생하는 경우를 살펴보면

$$P_{pair}(\text{mid point}) = ((N/2)*(N/2)) / {}_{N}C_{2} \approx 1/2$$

또한,

$P_{err(point)} = E_{net} * T_{change}$, $P_{tx} = \lambda_{tx} * T_{change}$

여기서,

E_{net} : error rate of the network

T_{change} : error가 발생한 시점부터 네트웍이 전환되기까지의 시간,

λ_{tx}: transmit frame arrival rate

E가 충분히 작고 T도 작은 값이므로 P_{error}는 매우 작다고 생각해도 좋다. 또한, 미리 system을 안정적으로 설계하여 E를 줄이는 노력이 필요함을 날 수 있다. 그리고, 서로간의 communication이 많은 station은 서로 인접하게 배치하면 P_{pair}의 값을 줄여서 결과적으로 P_{error}의 값을 줄일 수가 있다. 또한 T가 작아짐에 따라 P_{error}값이 작아질 수 있음을 관찰할 수 있다.

error발생시의 전송시간은 다음과 같이 생각된다.

T_{tx_error} ≡ error발생시 data가 전송되었을때 재전송을 포함해서 걸리는 시간

T_{tx} ≡ 평균 전송시간

T_{change} ≡ 네트웍을 전환하는데 걸리는 시간

이라고하면

$$T_{tx} + T_{change} \leq T_{tx\_error} \leq 2 * T_{tx} + T_{change}$$

로 볼 수 있다.

5. RedMAP의 구현

전체적인 전환 sequence를 살펴보면 다음과 같다.

①. error의 detection
- bus상의 ring이 깨지거나 각 NIU자체의 이상이 감지된 경우를 이상상태로 본다.
- 이 때, spare 네트웍에 대해서도 error가 발생하는 경우 '④' 번의 작업을 행해준다.

②. error의 broadcasting
- 이상을 발견한 NIU는 host에 알려주고 host는 spare 네트웍을 통해 broadcasting
- error broadcast가 수신된 NIU는 host에 알려준다.

* 이때, error broadcast의 conform이 필요하다.

③. 네트웍의 전환및 진행중인 작업들의 처리
- receive는 양쪽 NIU에서 하고 전송은 한쪽 NIU로만 하는 방식을 쓰면
네트웍 전환에서 생기는 data의 손실을 방지할 수 있다.
- 이때, error로 인해 발생하는 손실은 mini-MAP전체적으로 약간의 redundancy를 넣어서 re-transmit와 conformation을 통해 얻어질 수 있다.

④. 네트웍 disgnosis및 고장원인의 제거
- 각 NIU에서 error발생시 올라오는 개략적인 error의 report와 각 NIU의 diagnosis, 네트웍에 대한 diagnosis를 통해 error 발생 가능 부분을 찾아내고 이 부분에 대한 수리 작업을 한다.
- 수리가 끝나면 정상상태인지 확인한다.

⑤. 정상상태로의 복귀
- 복귀는 '③'번과 같은 방법으로 이루어 진다.

RedMAP은 ISL-Mini-MAP에, 다음의 ESM(error supervision machine), EMM(error management machine), ESH(error supervision host)가 결합된 형태로 이루어져 있다.

①. ESM(error supervision machine)
- MAC와 LLC에 걸쳐서 존재
- media와 NIU자신을 감시하여 error를 감지한다.
- error상황을 EMM에 보고하는 기능을 갖는다.
- EMM에서 내려오는 명령에 따라 각 detection machine을 disable 또는 enable, reset 등을 한다.
- EMM에서 broadcasting 명령이 내려올 경우 각 station에 broadcasting
- self-diagnosis기능 포함가능

②. EMM(error management machine)
- application 계층와 같은 level로 존재
- 네트웍의 전환및 전환시의 작업처리 담당
- ESM으로부터 error 상태가 감지되면, 먼저 자신의 주 네트웍(main-network)을 보조 네트웍(sub-network)으로 전환하고 전환된 사용 네트웍(active-network)을 통해 error message를 broadcasting한다.
- 자신의 동작 상황에 따라 ESM의 각 detection machine을 disable 또는 enable, reset 등을 한다.

③. ESH(error supervision host)
- error발생시에 error발생 부분을 찾고 이외에도 전체적인 네트웍의 관리 가능

error의 detection은 다음과 같이 여러 부분으로 나누어져 계층적으로 행해진다. 이때, 각 부분에서 error를 detect하면서, 가장 중요한 점은 error가 있는 것을 반드시 알아내어 host쪽에 알려 줄 수 있어야 한다는 점이다.

① TBC의 기능을 이용해서 media와 modem을 감시하고 MAC level에서 전송과 수신이 잘 이루어지는 지 감시하는 부분
② TBC의 동작이 잘 되고 있는지 감시하는 부분
③ NIU의 CPU가 살아 있는지 -즉, LLC가 살아 있는지 - 보는 부분
④ NIU와의 통신이 잘 이루어지는지 감시하는 부분

MAC에서의 error detection은 TBC(Token Bus Controler)의 기능을 이용하도록 하였다. 이것은 ISL Mini-MAP을 redundant하게 만들때 error detction machine을 구성하기 위해 추가로 드는 비용을 최소화 하기 위함이다. 본 연구에서 사용한 방식의 경우 맨 처음 시스템이 동작을 시작했을 때, 먼저 cable이 정상인지 모든 station이 살아있는지를 operator가 확인한 후에 다음의 error detection이 동작된다고 본다. 다음의 detection 방법들은 맨 처음 ring이 구성되기 이전에 네트웍 상에 문제가 있는 경우는 detection이 가능하지 않다.

cable 단락의 check은 ring이 재구성되는 시점을 포착하여 이루어 지는데, 이때 station이 추가되는 것은 checking sequence에 걸리지 않고, ring에서 빠져 나가는 것만을 걸리게 하면 의도적으로 빠져 나가고 싶을 때는 leave message를 보내고 난 후 빠져나가서 cable error checking sequence에서 제외시키고, 적절한 operation 후에 다시 들어오면 된다. 이 경우, 맨 처음 ring 을 구성하는 station만이 적절한 시간후에 - 즉 자기 스스로 ring의 구성이 완료 되었다고 생각된 후에 - cable error check 를 시작하면 된다. 이렇게 할 경우, 여러 station이 동시에 ring에 참여하는 경우 각자가 맨 처음 시작한 station이라고 생각하면 된다. 여기서, cable error check 시작 시점을 token이

돌기 시작하는 시점으로 한다. 그러면 station이 자기 혼자인 경우는 어차피 check가 필요 없고 2개 이상인 경우 ring이 구성된후부터 token이 돌므로 문제가 없다. 단, 애초 시작당시부터 문제가 있는 경우는 detect가 안된다. token이 도는것은 TBC statistics function의 number of token passed가 증가하기 시작하는 시점을 포착하여 알아낸다.

MAC부분의 error detection은 크게 세 가지로 나눈다. 즉, 첫째, logical ring에 이상이 있는 경우, 둘째, TBC에서 볼 때 modem혹은 media에 이상이 있다고 생각되는 경우, 셋째, TBC동작에 이상이 있다고 스스로 판단이 되는 경우이다.

logical ring에 이상이 있는 경우에 발생되는 상황을 다음의 세가지로 구분할 때, MAC의 station management 기능에 의해 일어나는 일을 TBC의 동작으로 살펴보면 다음과 같다[4][11].

①. 자신 바로 다음의 station이 빠져나갈 경우
- token_pass_failed -> who_follows

②. 자신 다음과 그 다음이 빠져 나갈 경우
- token_pass_failed -> who_follows -> who_follows -> solicit_any

③. 자신이외가 모두 빠져나갈경우
- token_pass_failed -> who_follows -> who_follows -> solicit_any -> idle -> bus_idle_timer_expired

④. 자신 바로 전 station이 token을 넘겨 주지 못하고 빠져나갈 경우
- bus_idle_timer_expired

따라서, TBC의 기능을 이용해 위의 상황이 발생할 때를 포착하는 것으로 위에 구분된 error를 detect할 수 있다.

또한, 앞서 구분된 세가지의 error중 TBC에서 볼 때 modem혹은 media에 이상이 있다고 생각되는 경우와 TBC동작에 이상이 있다고 스스로 판단이 되는 경우도 마찬가지의 방법으로 발견한다[11].

LLC 부분에서의 error detection 방법을 살펴보면, TBC가 command에 대한 결과를 주지 않을 때, MAC에 이상이 있는 것으로 판단하고, LLC자체의 오동작을 detect하기 위해서 별도의 watch dog timer를 설치한다. LLC는 주기적으로 watch dog timer를 strobe하여 계속적인 heart beat를 보내다. 이 때 watch dog timer는 이 heart beat를 듣지 못하게 되면 LLC의 error로 본다.

또한, LLC와 MMS를 연결해주는 DEP(Data Exchange Protocol)에서 LLC의 반응을 살펴보면서 interface의 이상 및 LLC의 이상을 감시한다[7][8].

ESM은 앞에서와 같은 방법을 통해 error를 detect하고, error가 발견되는 순간, 이 상황을 EMM에 알려 준다. 그러면, EMM은 사용 네트웍(active-network)을 주 네트웍(main-network)에서 보조 네트웍(sub-network)으로 전환시킨후, 이상 상태인 것을 broadcast할 것을 ESM에 요구한다. 다른 station들도 broadcasting을 받은 후, 이상 상태인것을 알아내어 주 네트웍(main-network)에서 보조 네트웍(sub-network)으로 전환하게 된다. 네트웍의 전환은 결국 사용중인 NIU를 전환하는 과정인데, 이것은 2개의 NIU에 각각 다른 번지를 지정하여 DEP에서 관련된 번지들을 main-NIU로부터 sub-NIU로 바꿔줌으로써 이루어진다.

네트웍 변환된 후에는 ESH에서 각 station으로부터 self-diagnosys된 data를 모으고, error 발생시에 얻어진 data와 error 발생후에 네트웍을 test하여 얻어진 data를 종합하여, 네트웍의 고장난 곳을 찾는다. 고장을 수리한 후 ESH는 각 station에 복구되었다는 message를 broadcast하여 다시 보조 네트웍으로부터 주 네트웍으로의 전환을 한다.

6. 결론

본 연구에서는 Mini-MAP의 일부를 이중화하여 네트웍이 고장나는 경우에도 정상적인 경우와 마찬가지로 동작이 가능한 Fault-tolerant MAP system인 RedMAP을 개발하였다. 대상이 되는 MAP system은 ISL-Mini-MAP으로 하여, NIU를 이중화시켰으며, 기존의 구조를 최대한 유지하는 방향으로 연구되었다.

RedMAP의 동작은 error의 detect, error의 broadcasting, 네트웍의 전환으로 이루어 진다. cable의 단락 상황이나 네트웍상의 다른 station의 송수신 기능의 이상은 token bus에서 행하여지는 station management기능을 간섭하여 알아낸다. 네트웍의 전환은 사용하는 NIU의 번지를 변경함으로써 이루어지고, 전환시에 진행중인 작업들의 동기(synchronization)는 한 쪽 NIU에 전송하고, 양쪽 NIU에서 수신하는 방법으로 해결한다.

고신뢰도 및 실시간제어를 필요로 하는 시스템에 RedMAP이 이용될 수 있다. 네트웍상에 이상이 있을 때에도 실시간특성을 그대로 유지하기 위해서는 이중화시키는 부분의 완전한 동기화, 보다 강력한 이상 상태 발견 기능등의 연구가 필요하다.

7. 참고 문헌

[1] 발전소 보일러의 디지탈 분산 제어 시스템 개발 및 적용 (*the development and application of digital distributed control system for boiler in the power plant*), 삼성 데이타 시스템 주식회사, 1991

[2] Jean-Michel Ayache, Jean-Pierre Courtiat, and Michel Diaz, "REBUS, A Fault-Tolerant Distributed System for Industrial Real-Time Control", *IEEE Trans. on Computers, Vol C-31, No. 7*, July 1982, pp637-647

[3] Michael G. Rodd, Farzin Deravi, *Communication Systems for Indusrial Automation*, Prentice Hall, 1989

[4] *IEEE standards for local area network. Token-passing bus access method and physical layer specifications*, IEEE, Inc.

[5] *IEEE Standards for Local Area Networks: Logical Link Control*, IEEE, Inc.

[6] *ISO 9506, Manufacturing Message Specification*, IEEE, Inc.

[7] 다수 기업 이중 기기간의 접속 장치 개발에 관한 연구, 서울대학교 자동화 연구소, 1990

[8] *MAP*을 이용한 공정 제어 시스템 개발, 자동화 연구소, 990

[9] *FA Network Mini-MAP*의 개발에 관한 연구, 서울대학교 공학 연구소, 1990

[10] *82511 Token Bus Modem User's Manual*, Siemens,

[11] *MC68824 User's MAnual*, Motorola, 1987