1999년도 대한전기학회 하계학술대회 논문집 1999. 7.19-21

SCADA 시스템의 FAILOVER SUBSYSTEM에 관한 연구

김영태, 조남빈 *
한국수자원공사 합천댐관리단

The study on Failover subsystem of SCADA system

Kim Young-Tae, Cho Nam-Bin*
Korea Water Resources Corp. Hap Chun Dam

Abstract

Failover subsystem of computer consists four modes In this paper,These modes will be discussed in more detail.

- dual computer mode
- failover mode
- single computer mode
- standby synchronization mode

we have suggested the method of dual/redunancy configulation of server computer. Failover is activated by the standby computer, active computer receives a failover request across the inter-computer link immediatly.The active computer controls the scada system and maintains the current state in it's data base and channel system safety.

1. 서 론

본 연구에서는 범용의 컴퓨터를 이용한 수력발전소의 SCADA시스템을 구축하면서 시스템의 안정과 신뢰도 향상을 위한 Failover system의 구축 사례에 대하여 수행 하였다.

최근의 계측제어시스템이 범용의 컴퓨터를 베이스로 하는 Open multi-vendor system으로 크게 변화하는데 반하여, 컴퓨터와 주변기기 및 응용소프트웨어등의 조합에 의한 시스템의 안정도 확보를 위한 Fail-over system의 도입 필요성이 대두된다.

SCADA 시스템의 효율적인 안정도 확보는 station-computer의 고장간격을 늘리거나 복구시간을 줄임으로써 증대시킬 수 있다. 고장간격은 SCADA 시스템에 의해 요구되는 컴퓨터 기능에 의해 주로 결정되며, 고장복구시간은 부품의 가용성과 시스템 구성의 이중화 정도에 따라 결정된다.

본 고에서는 시스템 고장에 의한 사고 및 손실을 최소화하고 신속 정확한 운영을 위해 요구되는 이중화 컴퓨터 구성(Dual computer configulation)에 대한 한국수자원공사 합천댐관리단에 적용한 사례를 중심으로 제시코자 한다.

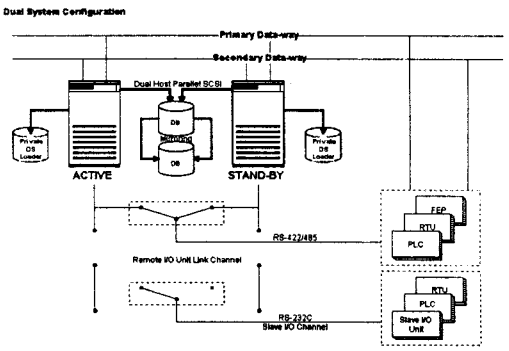
2. 본 론

2.1 장애(Error)에 대한 Dual/Redundancy 구성

본 시스템에 적용한 CCS(Centural Communication Server)는 시스템의 전체적인 관리 기능 및 데이터의 최종 관리를 담당한다. CCS의 장애는 전체 시스템의 최적 수행을 위해 배제되어야 할 요소이며 이를 위해 CCS는 Dual System 및 Data-way이중화의 구성을 갖추었다.

2.2 Dual System의 구성

Dual System은 Duplex/Redundancy 기능을 동시에 갖도록 구성된다. 이중화 System의 특징은 기능 손실의 존재와 고장을 일으킬 수 있는 요소를 없애기 위해 <그림 1.>과 같이 Remote I/O Unit 와의 Link channel의 공유 및 Data-way의 이중화 구성(Channel Duplication),



< 그 림 1. Dual system 의 구성 >

Data Base의 공유및 이중화(Data Base Duplication) 그리고 Non-stop operation의 진행을 위한 Processor간의 동기화와 Take-over 절차를 수행할수 있도록 구성된다. (Memory Synchronization/Take Over)

2.2.2 Channel Duplication

Dual System의 구성은 Remote I/O Unit(PLC, FEP, RTU, Slave I/O Unit ...)들의 Link Channel에 대해 양 시스템에서 공유 또는 절체에 의한 방법으로 제어 가능하도록 구성되어야 하며 LAN이나 RS-422/485 Channel은 이중 시스템에서 Data의 교신이 이루어 질수 있기 때문에 Channel을 논리적 구분으로 양 시스템에서 나누어 처리되고 항상 상대(peer)의 heart beat를 감지하여 없는 경우 상대의 Channel을 공유한다. 그러나 RS-232 및 Slave I/O Unit인 경우 Channel 절체가 따르기 때문에 Duplex에서 Channel을 논리적으로 나눠서 처리 될 수 없으며 절체의 제어를 통해 상대의 Channel을 수용해야 한다.

2.2.3 Data Base Duplication

- Hardware를 이용한 Data Base Duplication

두 개의 시스템에서 하나의 저장장치(Storage)를 공유케 하고 같은 용량의 Hard Disk를 이중으로 둬서 Mirror

ing 되게 하여 DB를 공유하면서 이중화되게 구성한다.

Hardware 환경으로는 "Dual Host Parallel SCSI Port"를 이용하며 이는 시스템의 Load를 줄이고 전체적인 시스템의 성능을 높이는 장점이 있는 반면 구성에 별도 Mirroing Device의 비용이 요구된다.

- S/W Data Base Duplication(Data Base Replication)

두 개 이상의 Server로 이용될 시스템에서 Back-up되어야 할 DB를 동시에 마련하여 다중화되게 구성한다.

이는 Network상의 시스템을 이용하기 때문에 별도의 Duplication Device 없이 다중화되는 잇점이 있지만 Data-way를 통해서 Access되어야 하기 때문에 Data량에 따라 통신부하(Network Communication Complexity)를 고려해야한다.

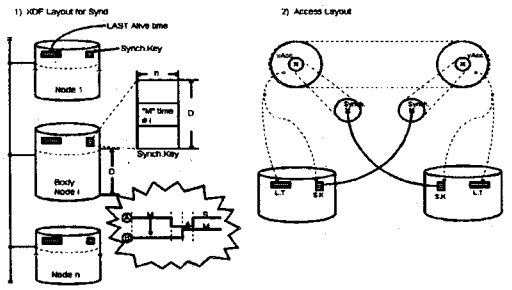
- Real-Time DB Duplication(TDF-Tag Define Form)

Load시 Master Server가 있을 경우 필요 정보 Dynamic Field만을 Copy한후 동기되며 없을경우엔 Master의 자격으로 동작된다.

- History DB Duplication (xDF)

History DB에 대한 Duplication은 Master Node와 Stand-By Node의 DB Replication에 의한 방법으로 이루어지며 이는 Master Node의 DB Write시 Stand-By Node의 DB에도 동시에 Update된다.

이 경우 Master와 Stand-By 사이의 DB Update에 대한 확인은 각 Node의 Synchronizing Table에 기록되며 Synchronizing Table은 Master Server와 Stand-By Node의 DB에 Update에 대한 확인과 동기를 위해 존재한다.



<그림 2. DB SYNCHRONIZING>

이들 DB의 동기화는 "<그림 2.>"에서 보이듯이 "XACC"와 "SYNCH" 두 개의 Thread에 의해 이루어지며 "XACC"는 Master Server와 모든 Stand-By Server Node의 동시 Update기능을 담당하며 "SYNCH"는 Update에 대한 동기를 맡는다.

2.2.4 Memory Synchronization(Processor-to-Processor Communication)

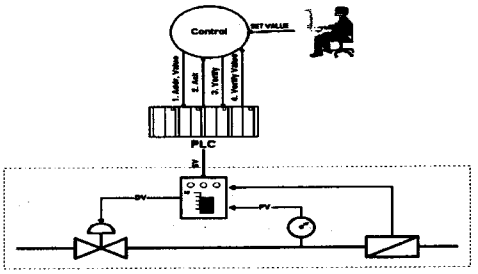
두 시스템간에 Task내의 공통 Data, Task와 Thread의 Input, Process 그리고 Data는 항상 같은 시점에서 Update 된다.

이는 이들 Data를 관리하는 Management System이 Node 내이든 밖이든 IPC(Inter Process Communication)에 의한 peer-to-peer 통신에 의해 가능하다.

<그림 3.>의"예"에서 Control 인 경우

input	: address, value
output	: verify value
process	: time#1, time#2

와 같은 상태로 Take Over 된다.



<그림 3. Memory Synchronizing>

Take Over System에서 1차적으로 Process 상태를 이어서 진행하고, 만약 Process 상태가 모호할 경우 Input Data를 다시 수행시키게 된다.

즉, Dual System에서 모든 Data는 IPC에 의해 Read / Write되게 하고, Load시 공통 Data는 Memory Application의 Take Over를 고려해 잡아 두고 해당 IPC Routine을 자신의 Node 뿐만 아니라 상대 Node Routine을 동시에 Call하여 둔다. 이런 경우 Network을 통한 Memory 동기 기능을 수행할수 있지만 이는 Processor의 Overhead가 크다는 것과 Network communication 속도에 의해 동기화 수행 Routine의 속도가 결정되기 때문에 빠른 Cycle time을 요구하는 Memory 동기에서는 문제점이 될 수 있으며 이를 위해 PCI Adapter를 사용한 Reflective Memory 혹은 Memory Channel 등의 별도의 Hardware 장비를 이용한 High Speed, Low Latency의 Shared Memory 기법을 사용 할수 있다.

2.2.5 Take Over

상대 Node에 자신의 Heart Beat를 항상 보내고, 상대 Node의 Alive 상태를 계속 점검한다. 여기서 Heart Beat라 함은 Time, Task Information 그리고 Resource 의 상태를 의미한다. 단지 상대 Node의 System이 On 상태에 있는 정도가 아니고 해당 Node 내의 모든 기능이 제대로 수행하는지에 대한 점검이다.

- System Alive Information

  일정한 Time Trigger에 의한 Node의 Alive Message를 전달한다. 상대방 Node의 System에 대한 On 상태 확인의 목적을 갖는다.

- Task Information

  상대방 Node의 System Task들의 정상수행 상태 검사를 위한 Task의 상태와 수행시간

등의 보고를 받는다. 이는 System On상태일 지라고 System의 정상 수행 상태에 대한 확인의 목적을 갖는다.

◦ Resource Information

상대방 Node의 System Resource(Memory, Thread ....)에 대한 상태와 한계치에 대한 검사를 함으로서 Take over의 상황을 결정한다. 이는 System의 안정적인 수행을 위한 예측의 목적을 갖는다.

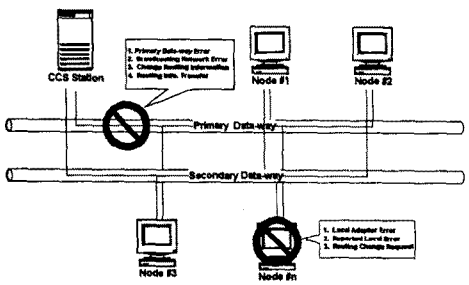
2.3 Data-way 이중화의 구성

일반 적인 분산처리 시스템에서는 Network을 기반으로 하고 있다. 각 Node간의 데이터는 Network Communication에 의해 이루어지며 Network 장애 발생시에는 시스템에 큰 손실을 가져올수 있으며 이런 경우 Network Backbone을 이중으로 구성하고 각 Node의 Network Adapter를 2중으로 장착하는 H/W Level의 이중화를 구성할수 있다. Network Backbone의 이중화는 물론 Application에서는 이런 이중화 환경을 인식하고 Network Line의 장애 혹은 Local Network Adapter 장애시에 Application은 능동적으로 Data-way의 Routing 변경과 보고가 있어야 한다.

2.4 Network 장애

2.4.1 Network Backbone의 장애

Network Backbone의 장애는 전체 Node의 Routing 정보의 변경을 요구하며 장애 복구시에는 사용자의 선택에 의해 Primary backbone과 Secondary Backbone의 선택이 요구된다.

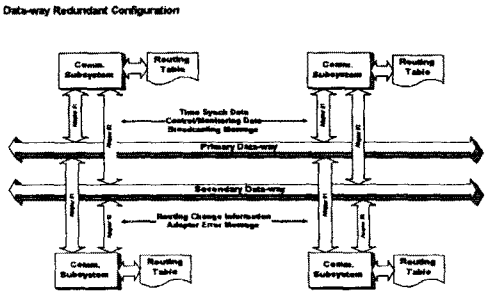


<그림 4. Network Backbone의 장애>

2.5.2 Local Network Adapter의 장애

Local Machine은 Data-way Routing table에 의해 동작하되 Network Adapter의 이상으로 인해 Routing table의 Primary backbone에 의해 동작할수 없을 경우 Secondary Backbone을 통해 Adapter 장애에 대한 보고(ALARM)를 행하며 전체 Routing Table의 변경을 요구한다.

각 Local Node에는 Data-way Communication을 위해 Data-way Routing table을 참조로하여 Communication을 담당하는 subsystem이 있으며 이는 Local Network Adapter 장애시 보고(ALARM)와 Routing table의 변경을 요구하는 역할을 담당한다.



<그림 5. Local Network Adapter의 장애>

Communication subsystem은 Network Communication 시점에 Routing table에 기록된 Logical address를 가지고 수행하며 Logical address의 변경은 CCS station에서 수행한다. CCS station은 시스템의 Routing table의 일치와 변경을 수행할수 있으며 Remote station으로 부터의 Routing 변경 요구에 응한다.

3. 결 론

이상에서 범용컴퓨터를 이용한 수력발전소 SCADA시스템의 이중화구성 설계시 고려되어야 할 Channel 및 DB의 Duplication방안 및 적용 원리등에 대하여 검토하였다. 본 연구의 실제 적용에 있어서 플랜트의 특성을 고려한 통합감시제어시스템의 구성은 현재 설계가 완료되어 부분적인 시공이 진행중이다. 분산되어 있는 두 개의 수력발전소 및 수문설비의 통합제어를 위한 광통신망을 통한 TCP/IP방식의 LAN(Local Area Network)의 도입과 근거리통신망 구축이 불가한 Remote I/O와는 별도의 Serial통신으로 플랜트설비의 통합제어방식의 제시 및 시스템 안정화 및 신뢰도 향상을 위한 Dual server의 적용등이 본 시스템구성의 주요한 특징으로 제시 될 수 있다.

[참 고 문 헌]

[1] 한국수자원공사,"현장자료전송을 위한 프로토콜 및 MMI표준화 연구",1997.12

[2]한국수자원공사,"합천댐 원격자동기록장치 운영 및 유지보수 매뉴얼",1999.03