고속 제어 처리 시스템 신뢰성 확보를 위한 이중화 시스템

이일화
LS산전

High reliability of fast control system based on changeover logic

YIL HWA LEE
LS Industrial System

ABSTRACT

고속 제어 처리 시스템의 신뢰성 확보를 위한 방법으로 시스템을 이중화로 구성한다. 이중화란 동일한 부품이나 장비로 구성하여 정상 동작 도중 오류가 발생하여도 다른 정상 부품 또는 장비로 하여금 정상 동작을 유지하도록 하는 것이다. 다양한 이중화 시스템의 구성 방안과 구조와 특징을 통해 시스템에 맞는 이중화 방안을 제안한다.

1. 서 론

고속 제어 처리 시스템의 정의는 시장 환경 마다 다르다. 공장에서는 ms 단위 제어를 고속이라 하고, 전력제어 시스템의 환경에서는 us 단위 제어를 고속이라 정의한다. CPU와 같은 프로세서와 전력전자반도체의 성장은 전력 제어의 단위를 us 단위로 끌어내렸다. us 단위의 고속 제어 시스템의 경우 정밀한 제어가 가능해진 만큼, 운영중인 시스템의 안정성과 신뢰성을 보장할 수 있게 되었지만 여전히 고장이 발생 했을 경우 취약점은 지니고 있다. 오히려 고속으로 제어는 고장 발생으로 인한 더 다양한 수의 오작동을 발생시킨다. 고장에 대한 신뢰성 확보를 위해서 대부분의 고속 제어 시스템은 이중화로 구성된다. HVDC와 SVC 같은 시스템을 고장이 발생하더라도 안정적으로 절체 되고 연속 운영이 가능한 최적의 이중화 구조를 제안한다.

2. 제어 이중화

1.1 Cold Standby

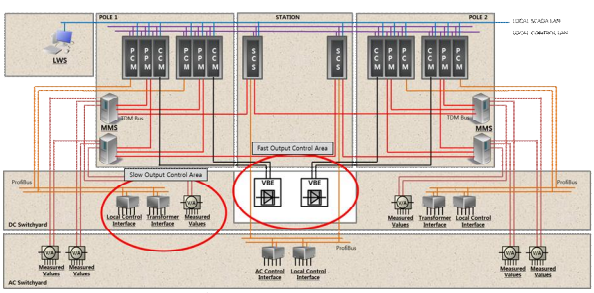
Cold Standby 이중화 방식은 가장 널리 사용되는 방법으로 두 개의 동일한 제어 시스템에서 하나의 시스템이 정상 동작하다가, 문제가 발생하면 다른 시스템이 기동을 시작한다. 문제가 발생한 제어 시스템으로부터 기존 동작 상태 정보들을 전달받아서 동작 주체가 되어 시스템을 제어한다. PLC나 DCS와 같은 ms 단위의 고속 제어 시스템에서 주로 적용되고 있다. 시스템 절체에 들어가는 시간은 10ms 정도 걸린다.

1.2 Hot Standby

이중화 고속 절체를 지원하는 방법으로 Hot Standby 방식이 있다. HotStandby 방식의 경우, 두 개의 제어 시스템이 항상 동시에 동작한다. 제어 시스템의 동작의 주체를 결정하는 것은 출력 여부다. 제어 시스템이 동작을 한다는 것은 시스템을 제어를 하는 권한이 있다는 의미이고, 제어에 대한 제어 명령 신호가 출력이 된다. HotStandby 방식에서는 두 제어 시스템이 동시에 동작을 하고, 제어 명령 신호를 동시에 출력하지만 제어 대상 장비는 하나의 제어 명령 신호를 받아서 처리한다. 동시에 출력되는 두 개의 제어 명령 신호를 순간적으로 판단하여 선택된 하나의 제어 명령 신호만 제어 대상 장비에 갈 수 있도록 하는 장비가 바로 COL(Change Over Logic 또는 SwitchOver Logic)이다.

1.2.1 Change Over Logic

COL은 HotStandby 방식의 이중화 기능을 지원하는 장비로 안정적인 이중화 절체 기능과 고속 절체 기능을 성공적으로 수행한다. COL은 동작하는 시스템의 상태 정보를 실시간으로 모니터링하며, 시스템 절체 여부를 판단한다. 시스템이 요구하는 절체 시간은 Fast Output Control의 성공적인 연속 제어를 위해 1ms 이내를 요구하고 있다.



<그림1> Fast/Slow Control Area

1.2.1.1 Slow Output Control

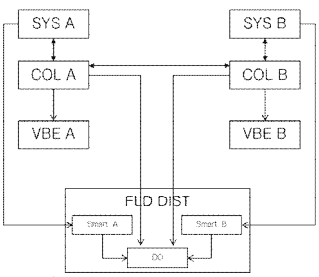
10ms이내의 딜레이가 발생해도 문제가 없는 대상 장비에 대한 제어 출력 명령이다. 사용자에 의한 제어 명령이나, 온도 제어와 같이 제어 반응이 느린 대상 장비에 사용되는 제어 명령이다. 사용자가 HMI에서 제어 명령을 조작하면, 제어 명령이 대상 장비로 전달되는데 HMI로부터 Software로 발생한 제어 명령이, 통신으로 제어 보드로 전달되고, 물리적 DO 장비의 동작신호로 변경되어 최종 대상 장비로 전달되는데 10ms 이내의 딜레이가 발생해도 문제 없는 경우 Slow Output Control이라 한다. 사용자에 의한 Switch On/Off 동작이 여기에 해당한다.

1.2.1.2 Fast Output Control

HVDC나 SVC와 같이 Phase 제어를 하는 경우 us 시간 단위의 제어 명령이 전달되고 수행된다. 이 경우 문제가 발생한 제어 시스템에서 다른 시스템으로 절체되는데 걸리는 시간을 최소화해야 시스템이 받는 충격을 최소화 하고, 시스템 동작을 안정적으로 유지할 수 있다. 시스템에서 요구하는 MAX 절체 시간을 1ms 이내로 하도록 한다. COL은 Slow/Fast Output Control 절체 성능을 만족시키기 위해서 1ms를 기준으로 제작 및 설계되어야 한다.

1.2.1.3 Single Mode COL System

COL을 포함한 이중화 시스템은 구조에 따라서 Single과 Multi Mode로 구분한다. Single 모드는 COL이 진단 기능과 함께 하며 A시스템에 관련된 모든 장비 및 시스템이 A에 한대 묶여서 동시에 절체가(그림2) 이루어 진다.



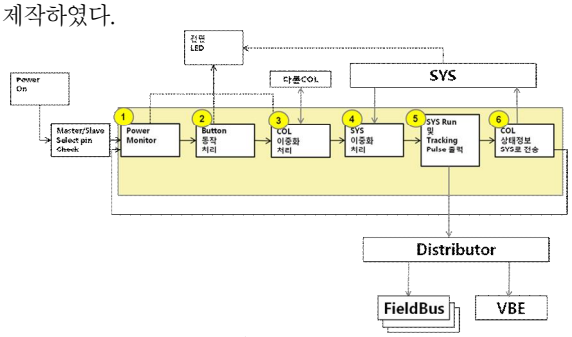
<그림2> Single Mode COL System

1.2.1.3 Multi Mode COL System

모든 시스템 및 제어 장비들뿐만 아니라, COL도 이중화로 구성되어 있다. 어떤 이중화 부분에서 고장이 발생하면 그 고장은 그 영역에만 국한되어 절체된다. 시스템 유연성이 매우 높지만, 로직 및 시스템 관계가 복잡해져서 구현하는데 난해함이 뒤따르며, 새로운 고장 발생 원인이 되어, 되려 신뢰성을 낮추게 된다. 그래서, 시스템의 특성과 개발자의 철학에 맞추어 복잡성과 단순성 적용 여부를 부분적으로 신중하게 판단해서 적용해야 한다.

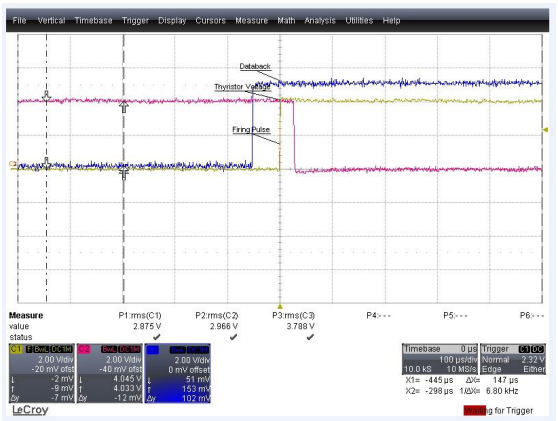
1.2.1 Change Over Logic Test

전류형 HVDC C&P H/W Platform을 설계함에 있어서 복잡성을 중간 레벨로 잡고 시스템을 구성하였다. 제어기와 COL까지는 Cross 이중화로 구성하고, VBE는 Simple Mode 이중화로 구성하였다. 그림3.은 HVDC 전류형에 적용한 COL의 동작 Flow를 나타낸다. FPGA로 아래 로직을 구현하여 COL을 제작하였다.



<그림3> COL Action Flow

실제 HVDC 전류형 시스템에서 측정한 절체 시간(그림4)으로, 절체 시간은 100us~400us에서 측정되었다. 성능은 목표 1ms 이내를 충분히 만족시켰으며, 시스템의 안정성과 신뢰성을 높였다.



<그림4> ChangeOver Logic 절체시간

3. 결론

이중화 시스템을 안정적으로 지원하기 위한 다양한 이중화 구조와 COL 기능이 있다. 이중화 시스템이 복잡할수록 시스템은 유연해지며, 고장이 동시에 발생해도 시스템의 안정성이 유지될 확률이 높다. 하지만, 이중화 시스템이 복잡해짐으로 인해서 개발 난이도가 올라가며 또 다른 고장 발생 요인으로서의 고장 조건이 늘어난다. 이중화 시스템의 구조가 간단하다면 개발 난이도도 낮아지며 유지 보수가 수월하지만, 동시에 발생하는 고장 대응에 취약하고, 다양한 고장에 대한 대처 방법에 한계가 있다. 시스템 신뢰성 측면에서 이중화는 당연히 갖춰야 할 시스템이지만, 신뢰성을 높이기 위한 COL 및 이중화 구조에 대한 연구는 계속되어야 한다.