이중안전장치(Fail Safe) 및 연동장치(Inter Lock)

1. 서론

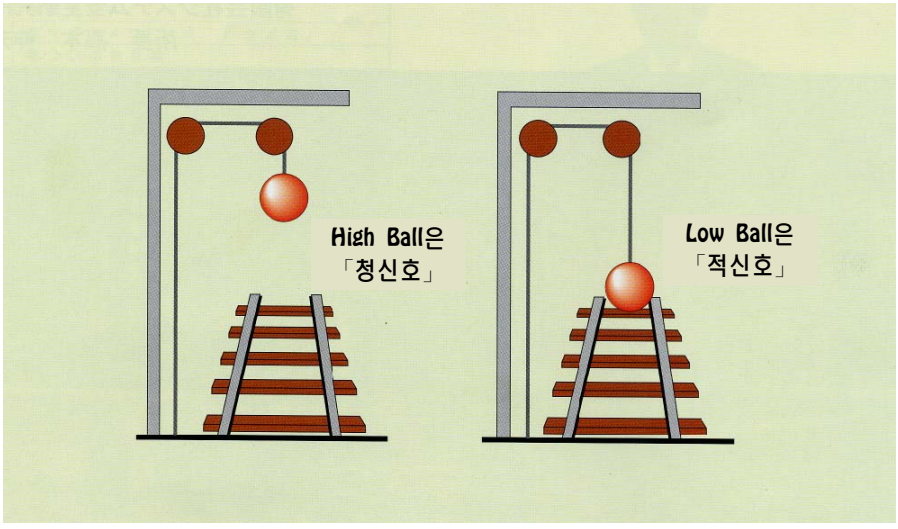
석유, 석유화학 또는 화학 등의 공정 플랜트는 가연성, 독성, 반응성을 가진 위험물질을 대량으로 보유 및 취급하고, 구성장치는 배관으로 연결되어 제어시스템에 의해 고도로 제어되는 대규모 시스템이다.

또한 플랜트는 인간과 기계의 Man · Machine System으로 장치의 고장 또는 오조작 등에 의해 비롯되는 사고발생의 잠재위험성을 가지고 있다. 안전을 확보하기 위해서는 다양한 접근방식이 필요하지만, 여기서는 안전 확보에 사용되고 있는 이중안전장치(Fail Safe)와 연동장치(Inter Lock) 방법을 소개한다.

2. 이중안전장치

JIS Z 4001(원자력용어, 1999년)에는 이중안전장치를(Fail Safe) 「설계상 원칙에 관한 것으로 부품과 시스템에 고장, 파손, 오동작이 발생해도 안전상태가 확보될 수 있는 것」으로 정의하고 있다.

이와 같이 공정장치에 고장이 발생한 경우에도 안전한 상태로 이행하는 것을 이중안전장치라고 한다. 이중안전장치의 방법으로서는 에너지가 높은 곳에서 낮은 곳으로 흐르게 되는 자연법칙에 기초한 방식이 바람직하다고 여겨진다. 자연법칙에 따른 이중안전장치의 알기 쉬운 예로서는 1830년대에 미국을 중심으로 사용되었던 철도신호를 들 수 있다.(그림 1 참조)



【그림 1】 철도신호의 이중안전장치

신호기는 기둥에 활차를 취부하고, 둥근 공에 설치된 망을 당겨 공을 상하로 위치시켜 신호로 삼았다. 공을 높게 위로한 상태를 「High Ball」이라 하여 청신호로 하고, 공을 낮게 한 상태는「Low Ball」로 하여 정지신호로 삼은 것이다. 이 시스템에서 망이 끊어진 경우에는 공이 낙하하여 정지신호가 되고, 열차 운행에 지장을 초래하게 함으로써 안전상태로 이행하게 된다. 만약, 「High Bal을 적신호」,「Low Ball을 청신호」로 한다면 열차를 정지하기 위하여 공을 들어 올렸을 때 망이 끊어진다면 공은 지상에 낙하한 결과 청신호가 되어 위험상태로 이행하게 된다.

공정 플랜트에 있어 계장용 공기의 힘으로 개폐를 작동하는 제어밸브에 이중안전장치의 개념을 도입할 수 있다. 계장용 공기를 동력원으로 하여 개폐하는 제어밸브가 계장용 공기를 상실시 개폐 작동방향은 3가지 종류가 있다. 하나는 계장용 공기의 압력을 스프링의 탄성력보다 크게 하여 밸브를 열리게 하는 것으로, 이 타입은 공기계통의 고장으로 공기압력이 소멸되면 스프링은 원상태로 복귀하려는 힘에 의해 닫힌 상태가 된다. 반대로 공기압력에 의해 밸브를 닫도록 하는 제어밸브는 공기압력의 상실 시에 열리게 된다. 또한 공기압력을 상실한 때에 개폐가 이전의 상태를 그 대로 유지하는 타입도 있다. 계장용 공기의 상실 시 제어밸브의 개폐 작동방향은 공정의 특성을 고려해서 안전 상태로 이행하도록 결정되지만, 냉각계통의 밸브는 開방향에, 가열계통의 밸브는 閉방향에 설정하는 것이 일반적이다.

3. 연동장치

연동장치(Inter Lock System)는 공정안전의 확보에 있어 매우 중요한 시스템이다. 연동장치에는 오조작방지를 목적으로 한 것과 공정에 이상이 발생한 긴급사태시에 펌프 및 컴프레셔 등 회전기계류의 정지, 긴급차단밸브의 작동, 반응기의 긴급압력방출 등 위험상태의 회피를 목적으로 한 공정안전 연동장치로 분류할 수 있다. 아래에 오조작방지 연동장치와 공정안전 연동장치 방법을 나타낸다.

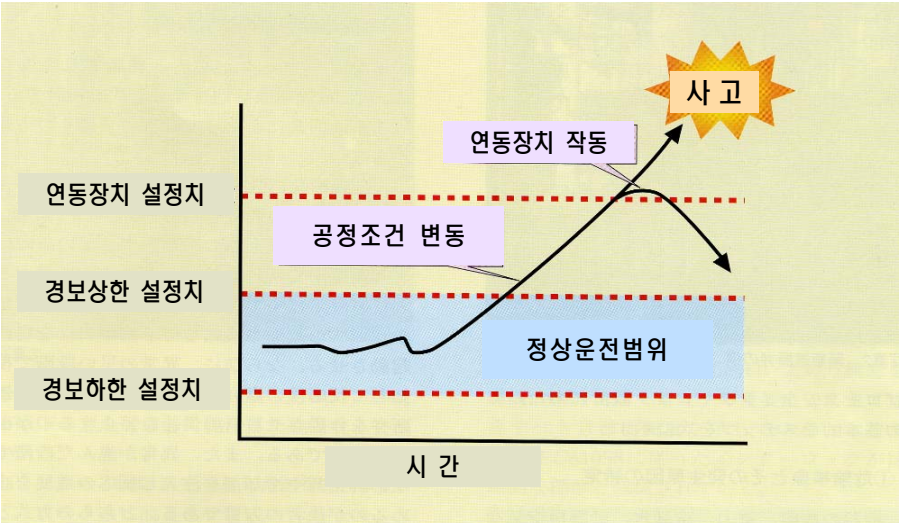
4. 오조작방지 연동장치

Foolproof는 「잘못해도 안전하게」라고 하는 설계 취지에 따라 잘못하는 것을 방지한다. 또는 운전원이 잘못으로 조작을 해도 동작되지 않도록 하는 방법이다. Foolproof의 수단 중 하나가 연동장치이다. 가장 단순한 연동장치는 수동조작밸브에 체인을 두르고, 작은 자물쇠로 채워 열쇠가 없으면 밸브를 조작할 수 없도록 하는 방식이다. 안전밸브의 주밸브와 평상시에 조작하지 않는 중요한 게이트밸브 등에 이 방식이 사용된다. 또한 기계가공설비와 고압프레스 등의 시스템은 운전 중에 사람이 접근하는 것은 매우 위험하다. 따라서 사람이 접근할 수 없도록 울타리와 문을 설치하여 문이 열려지면, 또는 울타리 안에 사람이 있는 것을 감지하면, 기계를 자동으로 정지시키도록 하는 연동장치가 설치된다.

공정 플랜트에 있어 오조작방지 연동장치의 예로서 보일러 점화 시의 폭발방지 연동장치를 들 수 있다. 보일러의 폭발사고는 연료 가스 및 기름이 로 내에 누설되고, 폭발성 혼합기체가 형성된 상태에서 버너에 점화를 시도할 때에 많이 발생한다. 폭발방지를 위해서는 버너 점화전 로 내에 공기를 송풍하여 배관에서 누설되어 체류하고 있을 지도 모르는 가연성가스를 배출한다. 보일러 점화시의 폭발방지 연동장치는 로 내를 통풍 팬에 의해 일정 시간 퍼지된 것을 확인하지 않으면 연료밸브가 열리지 않도록 한다. 또한 파일롯트 버너에 점화한 것을 확인하지 않으면 주버너의 밸브가 열리지 않는 시스템으로 하는 것이 일반적이다. 그 밖에 컴프레셔와 대형 펌프의 윤활유 계통의 유압과 냉각수 유량이 정격치에 도달하지 않는 경우에는 스위치를 켜도 기동되지 않는 시스템 등이 있다.

5. 공정안전 연동장치

공정 플랜트에 장치 고장과 오조작이 발생하면 압력, 온도 등 공정조건이 변동하여 한계치를 초월하면 장치를 손상 및 파괴하는 사고로 연결되는 위험성이 있다. 공정안전 연동장치는 공정 상태량이 정상운전범위를 큰 폭으로 초과할 때에 공정조건의 이상을 검지해서 긴급차단밸브 등을 작동시켜 플랜트의 안전을 확보하는 안전시스템이다.(그림 2) 공정안전 연동장치의 설계에 있어 기본적인 단계를 아래에 나타낸다.



【그림 2】 제어조건 변동과 연동장치

① 위험사상과 발생원인의 특정

장치의 고장, 전력, 냉각수, 계장용 공기 등의 유틸리티계통의 고장을 상정하고, 그것들이 어떤 위험사상 또는 사고로 연결되는가를 검토한다. 동시에 이러한 상황에 이르기까지의 시간, 위험사상의 중대도, 발생하기 쉬운 정도 등을 정리해서 기록한다. 그 검토결과를 토대로 연동장치가 필요하다고 생각되는 위험사상을 목록화한다.

② 운전대응으로 대처 가부 결정

목록화 된 위험사상을 운전원의 대응으로 방지할 수 있는지 여부를 검토한다. 운전대응으로 충분히 대처할 수 있다고 판단되는 경우에 연동장치는 필요가 없다.

③ 안전대책의 확인

상정된 위험사상에 대하여 물리적, 설비 구조면에서 안전대책이 강구될 수 있는지를 확인한다. 예를 들면 과압위험에 안전밸브가 설치될 수 있는가, 또는 내압설계를 할 수 있는가, 이상고온이라는 온도위험에서 예상되는 최고온도에 대응하는 재료가 선정될 수 있는가 등을 확인한다. 이런 대책이 충분하지 않는 경우에는 연동장치가 필요하다고 말할 수 있다.

④ 위험사상 회피방식 검토

연동장치가 필요하다고 판단된다면, 다음으로 위험사상을 회피하는 방식을 검토한다. 위험사상 회피에는 다음의 2가지 방식이 있다.

- 위험사상의 발생원인 차단
- 위험사상의 발전 저지

예를 들면, 발열반응기의 냉각수 펌프 고장에 의해 온도가 이상으로 상승하고, 그 대로 방치하면 폭주반응에 까지 발전하는 사태에서 냉각펌프의 고장을 검지하여 예비펌프를 자동 기동시킨다. 또한 이상의 초기단계에서 검지하여 반응성이 높은 원료공급라인의 긴급차단밸브를 작동시켜 원료의 공급을 정지하는 것이 전자의 대책이다. 또한, 이상이 발전한 단계에서 반응억제제 및 냉각제를 주입하여 반응의 발전을 억제하는 것이 후자의 대책이다. 어떤 방식으로 할지, 두 가지 방식을 조합할지는 위험사상의 특성을 고려하여 가장 효과적인 방법을 채용한다.

⑤ 연동장치의 기본구성 검토

위험사태 회피방식이 결정되면 그것을 구체화하기 위한 연동장치의 기본구성을 검토한다. 공정안전 연동장치는 센서, 로직솔바, 밸브 등으로 구성되어 있는 것이 일반적이다. 센서는 이상의 검출부이고 압력, 온도, 유량, 액위, 조성 등의 공정조건 가운데 어떤 이상을 검지해서 연동장치를 작동시키는 것이 좋은가를 결정한다. 또한 구동부에 있는 밸브를 어디에 설치할지를 검토한다. 변수가 선정되면 연동장치의 작동 설정치를 결정한다.

6. 연동장치의 신뢰성 확보

공정안전 연동장치는 보통 공정제어에 관여하지 않고, 공정이상이 발생했을 때 작동하는 待機계통의 안전시스템으로 공정제어계통과 물리적, 기능적으로 분리・독립시키는 것이 필요하다. 이 때문에 아래의 점을 고려하여 신뢰성을 확보할 필요가 있다.

(a) 공정제어계통에서 발생한 고장을 연동장치계통으로 파급시키지 않는다.

(b) 공정제어계통에서 설정치의 변경이 연동장치계통의 기능상실로 연결되지 않도록 한다.

(c) 공정제어계통과는 별도로 점검 및 보수를 한다.

(d) 공정제어계통과 연동장치계통의 공통요인 고장을 최소한으로 억제하고 연동장치계통의 신뢰성을 유지한다.

이를 위해서는 공정제어계통과 연동장치계통을 하드웨어 및 소프트웨어 양면에서 독립시킬 필요가 있고, 센서 및 구동부의 밸브 등은 공정제어계통과 겸용으로 하지 말고 독립시킨다.

구체적으로는

① 센서, 입출력장치, 최종 구성요소를 공정제어계통에서 분리한다.

② 논리기능 실행에 사용되는 하드웨어를 분리한다.

③ 시스템 소프트웨어를 분리한다.

④ 응용프로그램을 분리한다.

등이 요구된다.

또한, 연동장치는 공정의 안전확보에 있어 극히 중요한 시스템으로 상정된 위험사상의 중대도에 따라 높은 신뢰도가 요구된다. 연동장치의 신뢰성을 확보하기 위하여 국제전기표준회의(IEC)에서는 전기/전자/PES safety related system의 기능안전(Functional Safety)에 관한 국제규격 IEC61508을 발표했으며, 그것은 그대로 JIS화 되었다. 또한 미국계측기공업회는 공정산업에 대한 연동장치의 규격 ISA-S84.01을 발행하고, 연동장치의 설계에 관한 기본적인 절차를 담고 있다. 이들 규격에서 공통적인 것은 연동장치가 본래의 목적인 안전기능을 확실하게 수행하기 위하여 안전도수준(SIL : Safety Integrity Level)이라는 개념을 도입하고, 연동장치의 중요도에 대응해서 달성해야 할 목표 신뢰도를 나타내고 있으며, IEC61058을 따르는 연동장치가 국제적인 표준으로 인식되고 있다.

7. 결론

공정 플랜트에 국한되지 않고 기계가공, 철도, 항공기, 자동차 등에 있어서도 이중안전장치 개념, 연동장치의 채용은 폭넓게 시행되고 있으며, 안전확보 측면에서 대단히 중요한 개념 및 안전시스템이다.

참고자료 : Safety Engineering 133호(일본 종합안전연구소, 2005)

번역 및 편집 : 위험조사부 차장 김광섭