KOSHA GUIDE
P - 116 - 2012

경보시스템의 효율적인 관리에 관한 기술지침

2012. 8.

한국산업안전보건공단

안전보건기술지침의 개요

○ 작성자: 매경안전환경연구원 강 미진

○ 제 · 개정 경과

- 2012년 7월 화학안전분야 제정위원회 심의(제정)

○ 관련 규격 및 자료

- Chemical Information Sheet 6, "Better alarm handling", HSE, 2000
- HSG 48, "Reducing error and influencing behavior", 1999
- M L Bransby & J Jenkinson, "The management of alarm systems, CRR 166", HSE, 1998
- IEC 61511 Functional Safety - Safety Instrumented Systems for the process industry sector, First Edition, 2003
- IEC 61508 Functional Safety of electrical/electric/programmable electronic safety-related systems, Edition 2.0, 2010
- KOSHA Code, 방호계층분석기법에 관한 지침, 2012
- KOSHA Guide, 안전무결성등급(SIL)의 산정에 관한 지침, 2012

○ 기술지침의 적용 및 문의

이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈 페이지 안전보건기술지침 소관 분야별 문의처 안내를 참고하시기 바랍니다.

공표일자: 2012년 8월 27일
제 정 자: 한국산업안전보건공단 이사장

KOSHA GUIDE
P - 116 - 2012

경보시스템의 효율적인 관리에 관한 기술지침

1. 목적

이 지침은 최근 화학공장 등에서 이상상황이 발생하였을 때 이탈현상을 알리고 필요한 조치를 취하도록 설치된 경보시스템이 적절하게 관리되지 못하였을 때 발생할 수 있는 위험요인을 제시하고, 경보시스템을 효율적으로 관리하기 위하여 필요한 사항을 제시함으로써 화학공장에서의 사고피해를 최소화하는데 그 목적이 있다.

2. 적용범위

이 지침은 화학공장 및 이와 유사한 사업장에서 공정의 이상상태를 감지하기 위해 경보시스템을 설치, 운영하는 모든 경우에 적용한다.

3. 정의

(1) 이 지침에서 사용되는 용어의 정의는 다음과 같다

(가) “계장시스템 (Instrumented control system)”이라 함은 공정변수 및 상태를 감지하는 등의 역할을 수행하는 전기(Electrical), 전자(Electronic) 혹은 프로그래밍 전자시스템(Programmable electronic system) 등을 말한다.

(나) “안전계장시스템”이라 함은 하나 이상의 안전계장기능(Safety instrumented function)을 이행하기 위해 사용하는 계장시스템을 말하며, 일반적으로 감지부(Sensor), 로직해결기(Logic solver), 최종요소(Final element)로 구성된다.

(다) “로깅 (Logging)”이라 함은 필요한 결과, 예를 들어 공정변수 등과 같은 값을 일정한 간격으로 일지에 기록하는 것을 말한다.

(라) “휴먼인터페이스 (Human interface)”라 함은 계장시스템과 운전자를 연결시켜주는 것을 말하며, 흔히 모니터나 계기판 등의 시각적 접촉과 음성출력과 같은 청각적 접촉 및 근로자의 조작이 이루어질 수 있는 키보드, 마우스 및 터치화면 등을 포함한다.

(마) “플랜트인터페이스 (Plant interface)”라 함은 센서를 통한 입력, 액츄에이터(Actuator)를 통한 출력, 전선 등을 통한 통신 등을 말한다.

(바) “안전무결성등급 (Safety Integrity Level, SIL)”이라 함은 전기・전자・프로그램 가능형 전자장치로 구성된 안전관련 시스템이 정해진 시간에 모든 조건에서 특정안전기능을 만족스럽게 수행하는 확률의 범위를 4개의 불연속적인 수준으로 나타낸 것을 말한다.

(사) “작동요구 시 고장확률 (Probability of failure on demand, PFD)”이란 시스템이 특정한 기능을 작동하도록 요구받았을 때 실패할 확률을 말한다.

(2) 기타 이 지침에서 사용하는 용어의 정의는 특별한 규정이 있는 경우를 제외하고는 「산업안전보건법」, 같은 법 시행령, 같은 법 시행규칙 및 「산업안전보건기준에 관한 규칙」에서 정하는 바에 의한다.

4. 경보시스템의 중요성

4.1 계장시스템(Instrumented control system)

4.1.1 일반 사항

(1) 계기를 통한 제어시스템의 역할은 다음과 같다.

① 공정변수 및 상태에 대한 모니터링, 기록(Recording), 로깅(Logging)

② 공정변수 및 상태에 대한 정보 제공

③ 공정 상태를 변화시킬 수 있는 제어(Control)

④ 시운전, 정상운전, 비상정지 및 정상운전범위 내에서의 교란(Disturbance)

⑤ 위험요인 징후의 감지, 위험요인의 자동 종결 혹은 완화

⑥ 위험요인을 초래할 수 있는 자동 혹은 수동 작동의 방지

(2) 계장시스템의 기능은 경보와 공정제어시스템 및 보호시스템을 통해 이루어지며, 보호시스템이란 트립(Trip), 인터록(Interlock) 및 비상정지 등을 포함한다.

(3) 계장시스템은 휴먼인터페이스, 플랜트인터페이스, 논리구조, 부대설비 및 환경적 요인과 같은 요소를 공유하기도 하며, 독립적으로 운영되기도 한다.

4.1.2 안전계장시스템

(1) 계장시스템이나 장치가 다음의 특징을 가질 때 안전관련 기능을 갖춘 안전계장시

스템으로 인정된다.

① 공정이 제어를 벗어났을 때 동작

② 미리 정해진 안전상태로 이행

③ 통제나 제어가 가능한 상태로 유지

(2) 만일 안전계장시스템(Safety instrumented system)이 일반공정제어시스템(Basic process control system)과 분리되고 독립적으로 작동할 수 있는 경우에는 독립방호계층으로 인정할 수 있다.

(3) 안전계장시스템의 기능은 일반적으로 다음의 역할을 통해 달성될 수 있다.

① 위험요인의 초기사건 발생(Initiation) 방지

② 위험요인 징후의 감지

③ 위험한 사건을 종결하기 위해 필요한 조치의 수행

④ 위험요인으로 인한 결과의 완화

(4) 안전계장시스템은 그 기능의 요구빈도에 따라 다음과 같이 3가지로 구분된다.

① 안전기능의 작동이 요구되는 빈도가 1년에 1회 미만인 경우, 저요구형(Low demand mode)이라고 한다.

② 안전기능의 작동이 요구되는 빈도가 1년에 1회 이상인 경우를 고요구형(High demand mode)이라고 한다.

③ 안전기능의 작동이 실패하면 즉시 불안전한 상태를 초래하거나 다른 방호장치를 작동시켜야 하는 경우를 연속형(Continuous mode)이라고 한다.

(5) 저요구형(Low demand mode)일 경우 안전계장시스템이 보장하여야 하는 평균 작동요구 시 고장확률에 따라 안전무결성등급(Safety integrity level, SIL)은 <표 1>과 같이 4단계로 분류할 수 있다.

<표 1> SIL 분류

SIL	평균 작동요구 시 고장확률 (PFDavg)	리스크(Risk) 감소지수 (Risk reduction factor)
SIL 4	$< 10^{-4}$	$> 10^{4}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	10^{3} ~ 10^{4}
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	10^{2} ~ 10^{3}
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	10 ~ 10^{2}

(6) SIL의 구분 및 산정에 대한 일반사항은 KOSHA Guide 안전무결정등급(SIL)의 산정에 관한 지침을 참조하며, 위험성평가를 기반으로 공정에서 요구하는 SIL의 수준을 결정하기 위해 필요한 사항은 KOSHA Code 방호계층분석기법에 관한 기술지침을 참조한다.

(7) 안전계장시스템은 SIL 단계별로 그 기능과 역할을 유지할 수 있는 유지관리 수준이 달라지며, 특히 평균 작동요구시고장확률(PFDavg)는 다음에 따라 달라진다.

① 진단범위 (Diagnostic Coverage)

② 검증시험주기 (Proof Test Interval)

③ 검증시험범위 (Proof Test Coverage)

④ 공통원인지수 (Common Cause Factor)

⑤ 하드웨어고장허용치 (Hardware Fault Tolerance)

4.2 안전에 관련된 경보시스템의 역할

(1) 경보시스템은 운전자로 하여금 어떤 조치를 취하도록 함으로써 안전계장시스템의 동작빈도를 감소시키고 공정 전반의 안전을 향상시키는 역할을 수행한다.

(2) 안전계장시스템에 포함되는 경보시스템은 다음과 같이 관리되어야 한다.

① 해당 경보가 작동하였을 때의 대응절차를 문서로 명확하게 작성하고, 운전자를 훈련시켜야 한다.

② 해당 경보는 다른 경보와 구별이 가능하고, 우선순위를 가져야 하며, 경보가 작동되는 동안 계속 운전자가 관찰할 수 있어야 한다.

4.3 부적절한 경보시스템의 위험요인

(1) 공정의 비정상상태를 알리는 경보가 너무 많은 경우, 가장 중요한 조치가 필요한 것이 무엇인지 명확히 알 수 없다.

(2) 경보의 소리가 주변의 소음과 비슷한 수준이거나 경보의 색상이나 명도가 주변의 조명과 비슷한 수준인 경우, 근로자가 경보를 인지하기 어렵다.

(3) 근로자가 상주하는 곳이 아닌 장소에서 경보가 발생하면, 필요한 후속조치가 적절한 시기에 시행될 수 없다.

(4) 경보가 발생한 후 근로자의 후속조치에 필요한 시간이 충분히 확보되지 않으면 공정을 정상상태로 회복할 수 없다.

5. 경보시스템의 효율적인 관리방안

5.1 문제점 도출

(1) 다음 사항을 기준으로 현재 경보시스템의 현황을 파악한다.

① 얼마나 많은 경보가 설치되어 있는가?

② 모든 경보가 반드시 필요하며, 근로자의 후속조치가 필요한 것인가?

③ 정상 운전 중 경보 발생비율은 얼마인가?

④ 비정상상태에서 경보의 발생비율은 얼마인가?

⑤ 경보 지속시간은 어느 정도인가?

(2) 다음 사항을 기준으로 현재 경보시스템으로 인한 문제점을 파악한다.

① 과다한 경보로 인해 혼란을 초래한 적이 있는가?

② 연속적으로 짧은 시간 동안 사소한 경보가 발생한 적이 있는가?

③ 규칙적으로 경보 소리를 끄는 경우가 있었는가?

④ 경보의 우선순위가 있었다면 도움이 되었는가?

⑤ 근로자가 각각의 경보에 대한 후속조치를 잘 알고 있는가?

⑥ 경보가 울렸을 때 제어실 화면을 통해 얼마나 쉽게 해당 설비를 찾아낼 수 있는가?

5.2 경보시스템의 설계

5.2.1 적정한 경보 발생비율

(1) 정상 운전 중 근로자가 충분히 인지하고 조치할 수 있는 경보의 발생비율은 10분 동안 1개를 초과하지 않는 것이 바람직하다.

(2) 비상상황인 경우, 근로자가 충분히 인지하고 조치할 수 있는 경보의 발생비율은 정상조건을 벗어난 처음 10분 동안 10개를 초과하지 않는 것이 바람직하다.

5.2.2 경보의 선정 및 우선순위 부여

(1) 비상상황에서 오랫동안 울리는 경보나 오작동으로 인한 경보가 발생하지 않도록 설계한다.

(2) 근로자가 상주하는 지역이 아닌 곳에 경보를 설치할 필요가 있을 경우, 근로자가 상주하는 인근 지역에 해당 경보를 반복할 수 있는 장치(Repeater)를 설치하는 것이 바람직하다.

(3) 반드시 필요한 경보를 선정하였다면 근로자가 후속조치를 하지 못할 경우 예측되는 사고피해결과를 토대로 하여 우선순위를 결정한다.

(4) 경보의 우선순위는 대략 3단계로 구분하는 것이 바람직하며, 가장 중요한 경보는 전체 경보 중 약 5%, 중간 단계의 경보는 약 15%를 선정하는 것이 바람직하다.

5.2.3 경보의 소리와 밝기

(1) 경보는 주변의 일상적인 소음보다 약 10 dB 정도 높은 소리를 갖도록 하고, 경보가 울린 후 근로자가 소리를 줄일 수 있도록 하는 것이 바람직하다.

(2) 경보의 밝기는 예상되는 모든 외부 조건을 고려하여 결정하되, 주변과 쉽게 구별할 수 있는 색상을 선정하는 것이 바람직하다.

(3) 경보의 우선순위가 다르다면 소리, 음파, 색상, 깜박임 등을 적용하여 서로 구별이 가능하도록 설계한다.

5.2.4 경보 설정값의 결정

(1) 경보가 발생한 후 근로자가 충분한 조치를 취할 수 있도록 경보 설정값을 확인하

여야 한다.

(2) 필요한 경우 2단계로 경보를 구분할 수 있다. 예를 들어 High alarm 후 High-high alarm을 설정한다.

5.2.5 경보시스템의 지속적인 관리

(1) 경보의 우선순위를 선정하는 기준과 절차를 명확히 하고 모든 시스템에 대해 동일하게 적용하여야 한다.

(2) 새로운 경보를 설정하여야 하거나, 기존의 경보를 변경하여야 하는 경우에도 정해진 절차와 기준에 따라 경보의 우선순위를 결정하여야 한다.

(3) 운전이 정지된 설비나 공정은 경보시스템의 작동을 중지하여 불필요한 경보가 발생하지 않도록 한다.

5.3 교육 훈련

(1) 경보가 발생하였을 때 문제점을 쉽게 파악하고 필요한 조치를 취할 수 있도록 근로자를 교육시킨다.

(2) 경보가 발생하였을 때의 역할과 책임을 정상상황과 비상상황 각각에 대해 명확히 구분한다.

(3) 경보를 바이패스(Bypass)할 필요가 있을 때에는 반드시 정해진 절차에 따라 승인받은 후 조치하도록 하여야 한다.

<부록 1> 사고사례

1. 1989년 Phillips 66 사고사례 (미국 Passadena)

(1) 사고피해: 증기운 폭발 및 화재로 23명 사망, 약 300명 부상

(2) 사고개요: 폴리에틸렌 공장에서 반응기에 대한 예방정비 과정 중 인화성 물질이 누출되어 증기운 폭발을 일으켰고, 이로 인해 연쇄적으로 화재·폭발이 발생한 사고임.

(3) 경보에 관련된 문제점

경보의 소리가 너무 작아 공장 내 모든 사람이 경보가 울렸다는 것을 인지하지 못하였음.

2. 1994년 Texaco 정유공장 사고사례 (영국 Milford Haven)

(1) 사고피해: 26명 부상, 약 4천8백만 파운드의 손실

(2) 사고개요: 심각한 뇌우로 증류(Distillation) 및 알킬레이션(Alkylation) 공정 등에서 교란(Disturbance)이 발생하였고, 공정의 이상현상이 지속되는 과정에서 약 20톤의 인화성 물질이 플레어 넉아웃 드럼(Flare knock-out drum) 배출배관에서 누출되었다. 누출된 물질은 증기운을 형성하였으며, 드럼에서 약 110 m 떨어진 지점에서 점화되어 폭발한 사고임.

(3) 경보에 관련된 문제점

(가) 폭발이 발생하기 11분 전에 2명의 근로자가 인지하여 조치한 경보의 수량은 총 275개였음.

(나) 너무 많은 경보가 짧은 시간 동안 발생하였으며, 어떤 경보가 보다 중요한 지 알 수 없었으며, 무엇 때문에 경보가 발생하였는가에 대한 충분한 내용이 제어실에 표시되지 않았음.

(다) 근로자는 비상상태에 대처할 수 있는 훈련을 충분히 받지 못하였음.

3. 2003년 경기도 규산소다 제조공정 사고사례

(1) 사고피해: 3명 사망, 5명 부상, 공장 설비 붕괴

(2) 사고개요: 수산화나트륨, 물 및 규사를 용해조에 주입하고 규사를 용해하는 과정에서 용해로가 일정 압력에 도달하면 열 공급을 중단하여야 하나 열원 공급을 중단하지 못하여 용기 내에 높은 압력이 형성되고 이로 인해 용해조가 파열된 사고임.

(3) 경보에 관련된 문제점

(가) 내부 압력이 비정상적으로 상승하였으나 과압 방출장치인 안전밸브가 작동하지 않음

(나) 압력 상승 경보가 울렸을 때 무엇을 어떻게 하여야 하는지에 대해 공정운전자 등이 충분히 교육 받지 못하여, 대처가 미흡하였을 것으로 추정됨

4. 2005년 BP 정유공장 사고사례 (미국 Texas)

(1) 사고피해: 증기운 폭발 및 화재로 15명 사망, 180명 부상

(2) 사고개요: 정기보수를 마치고 이성화공정(Isomer unit)을 가동하기 위하여 시운전을 실시하는 중 탑에 설치된 계기의 오작동 등으로 인하여, 유입된 인화성 액체가 탑 상부까지 상승하여 압력방출밸브를 통해 블로우다운(Blowdown) 용기로 이송되었다. 용량을 초과하는 다량의 뜨거운 인화성 액체가 유입되면서 통기관(Vent)을 통해 대기로 방출되면서 증기운폭발이 발생한 사고임.

(3) 경보에 관련된 문제점

(가) 공정을 시작하기 전에 모든 경보를 작동하는 점검이 촉박한 시간 때문에 중단됨.

(나) 분리탑(Splitter) 액위에 대한 경보(High level alarm)이 작동하지 않아, 제어실 근로자가 적절한 대응을 할 수 없었음.

5. 2010년 BP Deepwater Horizon Platform 사고사례 (미국 멕시코만)

(1) 사고피해: 11명 사망, 17명 부상 및 해양오염

(2) 사고개요: 유정(Well)으로부터 시추라이저(Drilling riser)로 이송 중이던 고압의 메탄가스가 착암기(Drilling rig)로 누출된 후 점화되어 폭발한 사고임.

(3) 경보에 관련된 문제점

(가) 비상상황이 아니거나 중요하지 않은 사건에 대해서도 경보를 설정하여, 근로자가 너무 많은 경보에 노출됨.

(나) 중요하지 않은 경보가 너무 많아 취침시간에는 경보소리를 끈 상태로 유지하여, 사고 당일 비상상황에서 경보음이 울리지 않아, 스피커(Loudspeaker system)를 이용하여 상황을 서로에게 알려줌.

(다) 폭발성 증기운에 대한 경보는 몇 달 전부터 꺼진 상태였음.