KOSHA GUIDE

P - 113 - 2023

방호계층분석(LOPA)기법에 관한 기술지침

2023. 8.

한국산업안전보건공단

안전보건기술지침은 산업안전보건기준에 관한 규칙 등 산업안전보건법령의 요구사항을 이행하는데 참고하거나 사업장 안전·보건 수준향상에 필요한 기술적 권고 지침임

안전보건기술지침의 개요

○ 작성자 : 이 경 성
○ 개정자 : 이 근 원
한국산업안전보건공단 전문기술실 오상규

○ 제・개정 경과
- 2009년 9월 화공안전분야 제정위원회 심의
- 2009년 11월 총괄제정위원회 심의
- 2012년 7월 총괄 제정위원회 심의(개정, 법규개정조항 반영)
- 2023년 7월 화학안전분야 표준제정위원회 심의(개정, 법규개정조항 반영)

○ 관련규격 및 자료
- KS C IEC 61511-3, “프로세스 산업을 위한 계측 제어 시스템의 기능안전-3부”

○ 관련법규・규칙・고시 등
- 산업안전보건법 시행규칙 제50조(공정안전보고서의 세부내용 등)

○ 안전보건기술지침의 적용 및 문의
- 이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈페이지(www.kosha.or.kr)의 안전보건기술지침 소관 분야별 문의처 안내를 참고하시기 바랍니다.
- 동 지침 내에서 인용된 관련규격 및 자료, 법규 등에 관하여 최근 개정본이 있을 경우에는 해당 개정본의 내용을 참고하시기 바랍니다.

공표일자 : 2023년 8월 24일
제 정 자 : 한국산업안전보건공단 이사장

목 차

방호계층분석(LOPA)기법에 관한 기술지침

1. 목적

이 지침은 사업주가 수행하여야 할 공정위험성평가에 활용할 수 있는 기법 중 방호계층분석(LOPA)에 필요한 사항을 제시하는데 그 목적이 있다.

2. 적용범위

이 지침은 공정의 수명주기 동안 기본적인 설계 대안들을 검사하고 더 나은 종류의 독립방호계층(IPL)을 검토하는 것에 적용한다.

3. 용어의 정의

(1) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

(가) “방호계층분석기법 (Layer of protection analysis, LOPA)”이란 원하지 않는 사고의 빈도나 강도를 감소시키는 독립방호계층의 효과성을 평가하는 방법 및 절차를 말한다.

(나) “독립방호계층 (Independent protection layer, IPL)”이란 초기사고나 사고 시나리오와 관련한 다른 어떤 방호계층의 작동과는 관계없이 원하지 않는 결과로 전개되는 것으로부터 사고를 방호할 수 있는 장치나 시스템 또는 동작을 말한다. 독립적이라는 것은 방호계층의 성능은 초기사고의 영향을 받지 않고 다른 방호계층의 고장으로 인한 영향을 받지 않는다는 것을 말한다.

(다) “초기사고”란 원하지 않는 결과로 유도하는 시나리오를 개시시키는 사고를 말한다.

(라) “시나리오”란 원하지 않는 결과를 가져오는 사건이나 사건의 연속을 말한다.

(마) “기본공정제어 시스템 (Basic process control system, BPCS)”이란 공정이나 운전원으로 부터 나온 입력신호에 대응하는 시스템으로서 출력 신호를 발생시켜 공정이 원하는 형태로 운전되도록 하는 것을 말한다. 기본공정제어 시스템은 센서, 논리연산기, 공정제어기 및 최종제어요소로 구성되며 공정을 정상 생산범위 내에서 운전되도록 제어한다. HMI(Human machine interface)도 포함한다. 또한 공정제어시스템으로도 간주된다.

(바) “공통원인고장 또는 공통형태고장”이란 다중시스템에서는 동시고장을 야기하고 다중 체널시스템에서는 2이상의 다른 채널에서의 동시고장을 야기하여 시스템 고장으로 유도하는 하나 이상의 사고결과인 고장을 말한다. 공통 원인고장의 출처는 영향을 받는 시스템의 내부나 외부일 수 있다. 공통원인 고장은 초기사고 및 하나 이상의 방호장치 또는 여러 개의 방호장치의 상호관계를 포함할 수 있다.

(사) “최종조작요소 (Final control element)”란 제어를 달성하기 위하여 공정변수를 조작하는 장치를 말한다.

(아) “영향”이란 위험한 사고의 궁극적인 잠재적 결과를 말한다. 영향은 재해자수(사망자수), 환경이나 재산손실, 사업중단의 측면으로 표현된다.

(자) “논리해결기 (Logic solver)”란 상태제어 즉, 논리함수를 실행하는 기본 공정 제어시스템이나 안전계장시스템의 일부분을 말한다. 안전계장시스템의 논리해결기는 일반적으로 고장이 허용되는 프로그램 가능 논리제어기 (Programmable logic controller, PLC)이다. 기본공정 제어시스템상의 단일 중앙처리장치는 연속식 공정제어와 상태제어기능을 수행할 수도 있다.

(차) “작동요구시 고장확률 (Probability of failure on demand, PFD)”이란 시스템 이 특정한 기능을 작동하도록 요구받았을 때 실패할 확률을 말한다.

(카) “방호계층 (Protection layer)”이란 시나리오가 원하지 않는 방향으로 진행 하지 못하도록 방지할 수 있는 장치, 시스템, 행위를 말한다.

(타) “안전계장기능 (Safety iInstrumented function, SIF)”이란 한계를 벗어나는(비정상적인) 조건을 감지하거나, 공정을 인간의 개입 없이 기능적으로 안전한 상태로 유도하거나 경보에 대하여 훈련받은 운전원을 대응하도록 하는 특정한 안전무결수준(SIL)을 가진 감지장치, 논리해결장치 그

리고 최종요소의 조합을 말한다.

(파) “안전계장시스템 (Safety instrumented system, SIS)”이란 하나 이상의 안전계장기능을 수행하는 센서, 논리해결기, 최종요소의 조합을 말한다.

(하) “안전무결수준 (Safety integrity level, SIL)”이란 작동요구 시 그 기능을 수행하는데 실패한 안전계장기능의 확률을 규정하는 안전계장기능에 대한 성능기준을 말한다.

안전무결수준 운전상의 요구형태	평균 작동요구시 고장확률	위험도 감소
4	$\geq 10^{-5} \sim 10^{-4}$	$>$10,000 $\sim \leq$100,000
3	$\geq 10^{-4} \sim 10^{-3}$	$>$1,000 $\sim \leq$10,000
2	$\geq 10^{-3} \sim 10^{-2}$	$>$100 $\sim \leq$1,000
1	$\geq 10^{-2} \sim 10^{-1}$	$>$10 $\sim \leq$100

(2) 그 밖에 이 지침에서 사용하는 용어의 정의는 특별한 규정이 있는 경우를 제외하고는 산업안전보건법, 같은 법 시행령, 같은 법 시행규칙 및 산업안전보건기준에 관한 규칙에서 정하는 바에 따른다.

4. 일반사항

4.1 방호계층분석 팀 구성

(1) 방호계층 분석을 위한 팀은 다음과 같이 구성되어야 한다.

(가) 관련공정을 운전한 경험이 있는 운전원

(나) 공정 엔지니어

(다) 공정제어 엔지니어

(라) 생산관리 엔지니어

(마) 관련 공정에 경험이 있는 계장/전기 보수전문가

(바) 위험성평가 전문가

4.2 방호계층분석에 활용할 자료

(1) 팀 리더는 위험성평가의 목적과 범위를 정한 후 평가에 필요한 자료를 수집한다.

(2) 위험성평가에 사용되는 설계도서는 최신의 것이어야 한다.

(3) 기존공장의 위험성평가에 사용되는 설계도서는 현장과 일치되어야 한다.

(4) 방호계층분석에 필요한 자료 목록은 다음과 같다.

(가) 위험과운전분석 등의 정성적 위험성평가 실시 결과서

(나) 안전장치 및 설비 고장률 자료

(다) 인간실수율 자료

(라) 회사에서 별도로 정하는 위험허용기준(또는 규제당국에서 요구하는 기준)

(마) 공정흐름도면(PFD), 물질 및 열수지

(바) 공정배관・계장도면(P&ID)

(사) 공정 설명서 및 제어계통 개념과 제어 시스템

(아) 정상 및 비정상 운전절차

(자) 모든 경보 및 자동 운전정지 설정치 목록

(차) 유해・위험물질의 물질안전보건자료(MSDS)

(카) 설비배치도면

(타) 배관 표준 및 명세서

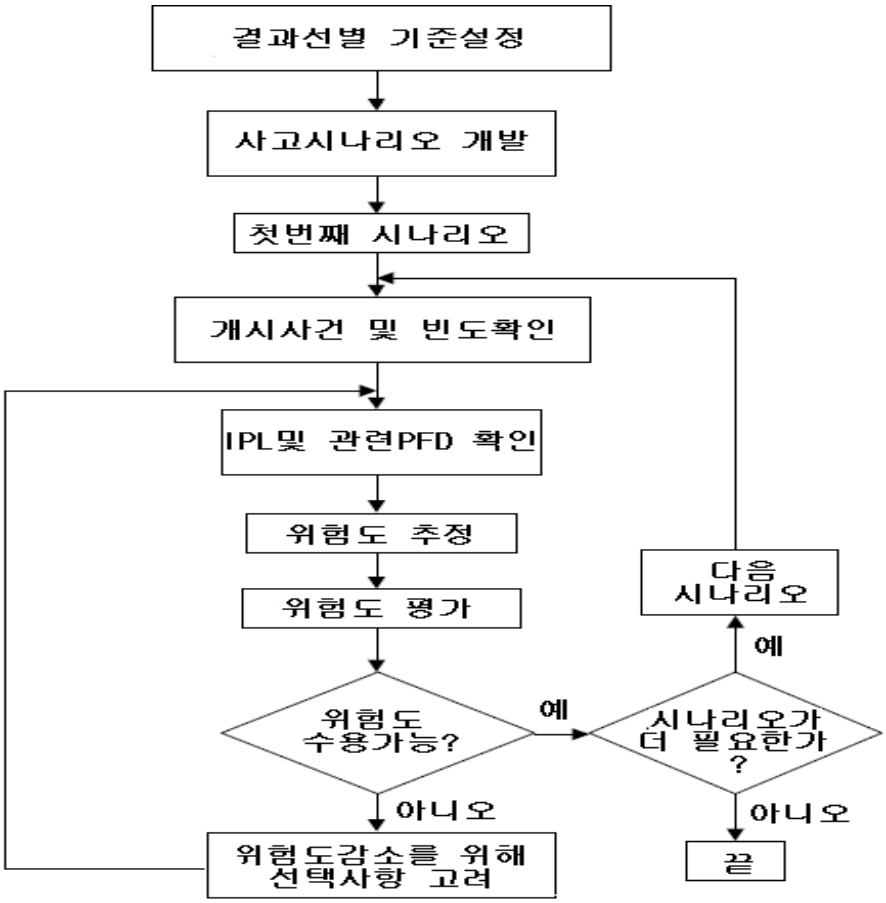
(파) 안전밸브 및 파열판 사양

(하) 과거의 중대산업사고, 공정사고 및 아차사고 사례 등

5. 방호계층분석 수행

5.1 방호계층분석 수행흐름도

방호계층분석을 위한 수행흐름도는 <그림 1>과 같다.



<그림 1> 방호계층분석 수행 흐름도

5.2 방호계층분석 단계별 수행절차

(1) 1단계-시나리오를 선별하기 위해 영향을 확인한다.

(가) 방호계층분석은 이전에 실시한 위험성평가에서 개발된 시나리오를 이용하여 평가한다.

(나) 방호계층분석 평가의 첫 번째 단계는 시나리오를 선별하는 것이다. 시나리오를 선별하는 방법은 영향을 기반으로 한다.

(다) 영향은 보통 위험과 운전분석 평가와 같은 정성적 위험성평가에서 확인한다.

(라) 다음으로 영향을 평가하고 그 크기를 추정한다.

(2) 2단계-사고 시나리오를 선택한다.

(가) 방호계층분석은 한 번에 한 시나리오에만 적용한다.

(나) 시나리오는 하나의 원인(초기사고)과 쌍을 이루는 하나의 결과로 제한한다.

(3) 3단계-시나리오의 초기사고를 확인하고 초기사고빈도(연간 사고수)를 정한다.

(가) 초기사고는 반드시 영향을 나타내어야 한다.(모든 안전장치가 실패한 경우)

(나) 빈도는 시나리오가 타당하게 적용될 수 있는 운전형태의 빈도와 같은 시나리오의 배경적인 면을 포함하여야 한다.

(다) 평가팀은 방호계층분석 결과와의 일관성을 얻기 위해 빈도를 평가하는 것에 관한 지침을 별도로 만드는 것이 필요하다.

(4) 4단계- 독립방호계층을 규명하고 각 독립방호계층의 작동요구시 고장확률을 평가한다.

(가) 몇몇의 사고 시나리오는 하나의 독립된 방호계층만을 필요로 하고, 다른 사고 시나리오는 시나리오에 대한 허용가능한 위험을 얻기 위해 많은 독립방호계층 또는 아주 낮은 작동요구시 고장확률을 가진 독립방호계층을 필요로 한다.

(나) 주어진 시나리오에 대해 독립방호계층의 필요조건을 충족하는 기존의 안전장치를 알아내는 것이 방호계층분석의 핵심이다.

(다) 평가팀은 평가시 사용할 수 있도록 이미 결정된 독립방호계층값들을 준비하여야 한다. 따라서 평가팀은 분석 대상인 시나리오에 가장 잘 맞는 값을 선택할 수 있다.

(5) 5단계- 영향, 초기사고, 독립방호계층 데이터를 결합하여 시나리오의 위험을 수학적으로 평가한다.

(가) 사고 영향의 정의에 따라 다른 요소들도 계산 과정에 포함할 수 있다. 접근 방법에는 산술적 공식과 그래프식의 방법이 있다.

(나) (가)항의 방법과는 상관없이 평가팀은 결과를 문서화하는 표준형식을 자체적으로 만들어 사용할 수도 있다.

(6) 6단계- 시나리오에 관련된 결정에 도달하기 위한 위험도를 평가한다.

(가) 방호계층분석으로 위험도 결정을 해야 하는 방법을 기술한다.

(나) 이 방법은 시나리오의 위험을 사업장의 허용위험기준이나 관련된 목표와의 비교를 포함하여야 한다.

5.3 방호계층분석 수행에 필요한 정보

(1) 방호계층분석에 필요한 정보는 위험과 운전분석 평가에 의해 개발되고 수집된 자료를 기본으로 하여 수행한다.

(2) 방호계층분석에 필요한 자료와 위험과 운전분석 평가 동안에 개발된 자료와의 관계는 <표 1>과 같다.

<표 1> 방호계층분석을 위한 위험과운전분석 개발 자료

방호계층분석(LOPA)에 필요한 정보	위험과 운전분석(HAZOP) 개발 정보
영향 사고	영향
강도 수준	영향강도
초기사고 원인	원인
초기사고 빈도	원인발생 빈도
방호계층	기존 안전장치
추가적인 완화대책	권고하는 새로운 안전장치

(3) 평가팀은 방호계층분석 대상 시나리오를 선정한 후 <별지서식 1>의 방호계층 분석 기록지를 작성한다.

5.4 방호계층분석 보고서에 포함될 사항

(1) 방호계층분석 보고서에는 다음과 같은 사항이 포함되어야 한다.

(가) 영향

(나) 강도수준

(다) 개시원인

(라) 초기사고빈도

(마) 방호계층

(바) 추가적인 완화대책

(사) 독립방호계층

(아) 중간사고빈도

(자) 안전계장기능 무결성수준

(차) 완화된 사고빈도

(카) 전체위험도

5.5 방호계층분석 보고서 작성

<별지서식 1>는 방호계층분석 수행동안에 필요한 작성 양식을 나타낸 것이다.

(1) 영향

위험과운전분석 평가에서 결정한 각각의 영향에 대한 설명은 <별지서식 1>의 제1항에 입력한다.

(2) 강도수준

강도 수준은 <표 2>와 같이 영향에 따라 미약, 심각, 매우 심각으로 구분하여 결정하며 <별지서식 1>의 제2항에 입력한다.

<표 2> 영향사고 강도 수준

강도수준	영향
미약	넓은 지역에 영향을 미칠 수 있는 잠재성을 가진 영향은 처음에는 국소지역으로 제한된다.
심각	영향사고는 공정지역이나 공정 외곽지역에 심각한 부상이나 사망을 유발할 수 있다.
매우 심각	심각한 사고보다 5배 이상인 영향 사고

(3) 개시원인

(가) 모든 영향사고에 대한 개시원인을 <별지서식 1>의 제3항에 기입한다.
(나) 영향사고는 많은 개시원인을 가질 수 있으며, 모든 개시원인을 나열하는 것이 중요하다.

(4) 초기사고빈도

(가) 초기사고의 빈도값은 연간 사고건수로 표현하며 그 값을 <별지서식 1>의 제4항에 기록한다.

(나) 일반적인 초기사고 빈도값은 <표 3>을 이용하여 구한다.

(다) 팀의 경험이 초기사고빈도를 결정하는데 있어 매우 중요하다.

(5) 방호계층

(가) <그림 2>는 일반적인 공정산업체에서 제공될 수 있는 다중 방호계층을 나타낸다. 각각의 방호계층은 다른 방호계층과 연관하여 작동하는 장치나 행정적인 제어의 결합으로 구성되어 있다. 높은 신뢰도를 가지고서 기능을 수행하는 방호계층은 독립방호계층으로서 인정이 된다.

(나) 초기사고가 발생하였을 때, 영향사고의 빈도를 감소시키기 위한 공정설계는 <별지서식 1>의 제5항에 기록한다. 이에 대한 예는 자켓(Jacket) 파이프 또는 자켓 Vessel이 될 수 있다. 자켓은 자켓 내부 배관이나 자켓 내부 Vessel의 무결성이 타협되면 공정물질의 누출을 예방할 수 있다.

(다) 기본공정제어 시스템은 <별지서식 1>의 제5항에 기록한다.

(라) 기본공정제어 시스템의 제어루프에서 초기사고가 발생하였을 때 영향 사고를 예방한다면 제어루프의 PFD_{avg}(작동요구시 고장확률)에 근거한 인정점수(Credit)를 받게 된다.

(마) 운전원에게 경보를 발하고 운전원의 개입을 활용하는 경보설비에 대한 인정은 <별지서식 1>의 제5항에서의 마지막 항에 작성한다.

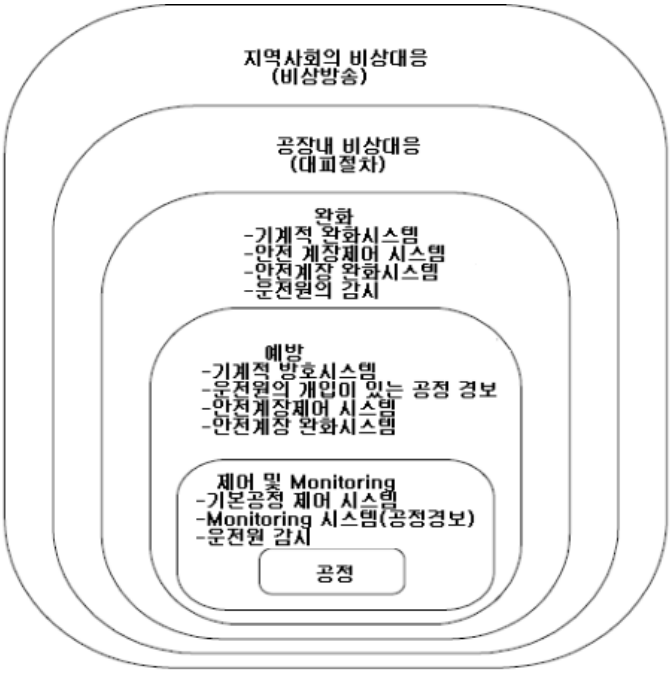
(바) 일반적인 방호계층의 PFDavg 값은 <표 4>에서 구한다.

<표 3> 초기사고 빈도

저	설비의 예상 수명기간동안에 매우 낮은 발생확률을 가진 고장이나 연속적인 고장 보기 - 3개 이상의 동시적인 계장의 고장이나 인간오류 - 하나의 탱크 또는 공정용기의 자체고장	$f < 10^{-4}$, /yr
중	설비의 예상 수명기간동안에 낮은 발생확률을 가진 고장이나 연속적인 고장 보기 -이중의 계장이나 밸브고장 -계장설비고장과 운전원 실수의 결합 -작은 공정배관이나 피팅류의 단일고장	$10^{-4} < f < 10^{-2}$, /yr
고	설비의 예상 수명기간동안에 합리적으로 발생한다고 예상되는 고장 보기 -공정 누출 -단일 계장이나 밸브고장 -물질의 누출을 야기할 수 있는 인간실수	$10^{-2} < f$, /yr

<표 4> 일반적인 방호계층(예방 및 완화)의 작동요구시 고장확률

방호계층	작동요구 시 고장확률
제어 루프	1.0×10^{-1}
인적 오류(훈련, 스트레스 받지 않음)	1.0×10^{-2} 부터 1.0×10^{-4}
인적 오류(스트레스 상황)	0.5에서 1.0
경보에 대한 운전원의 대응	1.0×10^{-1}
내부 및 외부의 압력을 받고 있는 상황에서 최대발생 압력이상으로 계산된 용기압력	10^{-4}이상(용기의 무결성이 유지된다면, 즉 부식을 알고 있고 검사나 정비가 예정대로 수행된다면)



<그림 2> 공정설비에서 발견되는 일반적인 위험감소방법

(6) 추가적인 완화대책

(가) 완화계층은 일반적으로 기계설비, 구조물, 절차 등과 관련하며 그 예는 압력방출장치, 방류둑(Dike, Bund), 출입제한 등과 같다.

(나) 완화계층은 영향사고의 강도를 감소시킬 수는 있지만 발생자체를 예방할 수는 없다. 그 예는 화재나 연기발생을 위한 Deluge시스템, 연기 경보시설, 대비절차 등이다.

(다) 평가팀은 모든 완화계층에 대하여 적절한 작동요구 시 고장확률을 결정하여야 하며 그 결과를 <별지서식 1>의 제6항에 작성한다.

(7) 독립방호계층

(가) 독립방호계층에 대한 기준을 만족하는 방호계층은 <별지서식 1>의 제7항에 나열한다.

(나) 방호계층을 독립방호계층으로서 인정하기 위한 기준은 다음과 같다.

① 방호계층은 확인된 위험을 최소 100배 이상 감소할 수 있어야 한다.

② 방호기능은 0.9이상의 유용성(Availability)을 제공할 수 있어야 한다.

③ 다음과 같은 중요한 특성을 지녀야 한다.

㉮ 구체성: 하나의 독립방호계층은 하나의 잠재된 위험한 사고의 결과를 유일하게 예방하거나 완화할 수 있도록 설계되어야 한다(예를 들면, 반응폭주, 독성물질 누출, 내용물 손실, 화재 등). 다중원인이 같은 위험한 사고를 유도할 수 있다. 따라서 다중사고 시나리오는 하나의 독립방호계층 작동을 개시할 수 있다.

㉯ 독립성: 하나의 독립방호계층은 확인된 위험과 관련된 다른 방호계층으로부터 독립적이다.

㉰ 신뢰성: 독립방호계층은 무엇을 위해 설계되었느냐에 따라 달라지므로 우발(Random)고장이나 시스템고장 형태 양쪽 다 설계에서 간주되어야 한다.

㉱ 확인가능성: 방호기능의 정기적인 정상작동을 입증하기위해 설계하며 입증시험과 안전시스템의 정비가 필요하다.

(8) 중간사고빈도

(가) 중간사고빈도는 초기사고빈도에 방호계층과 완화계층의 작동요구 시 고장 확률(<별지서식 1>의 항목 5, 6, 7)을 곱하여 구한다.

(나) 계산된 수치는 연간 사고건수로 표시되며 <별지서식 1>의 제8항에 입력한다.

(다) 중간사고빈도가 사업장에서 규정한 강도수준의 사고 기준보다 적다면 추가적인 방호계층은 필요가 없다. 그러나 경제적으로 적절하다면 추가적인 위험감소대책은 적용되어야 한다.

(라) 특정 시나리오에 대한 일반적인 중간사고의 빈도는 식(1)과 같이 계산한다.

$$f_i^c = f_i^I \times \prod_{j=1}^{j} PFD_{ij} = f_i^I \times PFD_{i1} \times PFD_{i2} \times \cdots \times PFD_{ij} \quad \cdots\cdots\cdots\cdots\cdots\cdots (1)$$

여기서,

f_i^c는 초기사고 i에 대한 결과 C의 빈도이다.

f_i^I는 초기사고 i에 대한 초기사고빈도이다.

PFD_{ij}는 초기사고 i의 결과 C에 대해 방호하는 j번째 독립방호계층의 작동요구시 고장확률이다.

(마) 중간사고빈도가 회사에서 규정된 강도수준의 사고 기준보다 크다면 추가적인 완화대책이 필요하다.

(바) 안전계장시스템형태로 추가적인 방호대책을 적용하기 전에 본질적으로 더 안전한 방법과 해결대책을 고려하여야 한다.

(사) 만약 본질적으로 안전한 설계변경이 가능하다면 <별지서식 1>은 수정되어야 하고 중간사고빈도는 회사의 허용기준 이하인지를 결정하기 위해 다시 계산하여야 한다.

(아) 앞의 시도가 중간빈도를 회사의 위험허용기준이하로 감소시키는 것이 어렵다면 안전계장시스템이 필요하다.

(9) 안전계장기능 무결성수준

(가) 새로운 안전계장기능이 필요하다면 필요한 무결성 수준은 사고의 강도수준에 대한 회사의 허용기준을 중간사고빈도로 나누어서 다시 계산할 수 있다.

(나) 이 수치보다 낮은 안전계장기능에 대한 PFD_{avg}는 안전계장시스템에 대한 최대치로서 결정하고 <별지서식 1>의 제9항에 입력한다.

(10) 완화된 사고빈도

(가) 완화된 사고빈도는 <별지서식 1>의 제8항과 제9항을 곱해서 다시 계산하고 그 값을 제10항에 입력한다.

(나) 이렇게 계속해서 평가팀은 확인가능한 각 영향사고에 대한 완화된 사고빈도를 계산할 때까지 계속한다.

(11) 전체 위험도

(가) 마지막 단계는 같은 위험성이 있는 심각하거나 매우 심각한 범위의 영향사고에 대한 모든 완화된 사고빈도를 합한다. 예를 들면, 화재를 발생시키는 모든 심각하거나 매우 심각한 영향사고에 대한 완화된 사고빈도는 합해져서 식(2)와 같이 이용한다.

$$f_i^{fire\ injury} = f_i^I \times [\Pi \prod_{j=1}^{J} PFD_{ij}] \times P^{ignition} \times P^{person\ present} \times P^{injury} \quad \cdots\cdots\cdots\cdots (2)$$

여기서,

$f_i^{fire\ injury}$=화재로 인한 사망 위험

$f_i^I \times [\Pi \prod_{j=1}^{J} PFD_{ij}]$ =누출된 모든 인화성물질의 완화된 사고빈도

$P^{ignition}$ = 점화확률

$P^{person\ present}$ = 그 지역에 사람이 있을 확률

P^{injury} =화재로 치명상을 입을 확률을 나타낸다.

(나) 독성물질을 누출시키는 모든 심각하거나 매우 심각한 범위의 영향사고를 합한 후에 식(3)과 같이 이용한다.

$$f_i^{toxic} = f_i^I \times [\Pi \prod_{j=1}^{J} PFD_{ij}] \times P^{person\ present} \times P^{injury} \quad \cdots\cdots\cdots\cdots\cdots\cdots (3)$$

여기서,

f_i^{toxic}= 독성물질 누출로 인한 사망위험

$f_t^{I_t} \times [\Pi \prod_{j=1}^{J} PFD_{ij}]$= 누출된 모든 독성물질의 완화된 사고빈도

$P^{person\,present}$= 그 지역에 사람이 있을 확률

P^{injury} = 누출로 인해 치명상을 입을 확률을 나타낸다.

(다) 위험성평가팀의 전문성과 지식이 공정설비의 조건과 작업, 영향지역에 대한 공식에서 요인들을 보정하는데 있어서 중요하다. 이 과정으로부터 공정에 대한 전체 위험은 이 공식을 적용하여 얻어진 결과를 합해서 결정할 수 있다.

(라) 만약 이 결과 영향을 받은 사람들에 대한 사업장기준을 만족하거나 작다면 방호계층분석은 완료된다. 그러나 영향을 받은 사람들이 다른 기존 설비나 새로운 프로젝트로부터 나온 위험에 따라 다를 수도 있기 때문에, 경제적으로 수행가능하다면 추가적인 위험 완화 및 감소를 시키는 것이 필요하다.

<별지서식 1> 방호계층분석 결과서 양식

#	1	2	3	4	5			6	7	8	9	10	11
					방호계층								
순서	영향 설명	강도 수준	초기 사고 원인	초기 사고 빈도	일반적인 공정 설계	기본 공정 제어 시스템	경보 등	추가적인 완화 대책, 접근 제한 등	독립방호 계층, 추가적인 완화대책, 다이크, 압력방출	중간 단계의 사고 빈도	안전 계장 기능 무결 수준	완화된 사고 발생 빈도	비고
1													
2													
N													

<부록>

방호계층분석방법 예시

다음은 위험과운전분석평가(HAZOP)에서 확인된 하나의 영향사고를 평가하는 방호계층분석방법의 예시이다.

1. 영향사고와 강도 수준

- 회분식 중합반응기에 대한 위험과운전분석(HAZOP)평가에서 고압을 이탈로 선정하였다.
- 스테인리스 스틸 반응기가 FRP탑 및 스테인리스 스틸 콘덴서로 연속으로 연결되어 있다.
- FRP탑의 파열은 점화원만 존재한다면 화재발생의 가능성이 있는 인화성 증기를 배출할 수 있다.
- 영향사고는 그 지역에서의 심각한 상해나 치명상을 유발하기 때문에 방호계층분석 팀은 <표 2>를 이용하여 심각도 수준의 엄격성을 선정하도록 한다.

2. 개시원인

- 위험과운전분석 평가결과 고압이라는 이탈에 대하여 콘덴서의 냉각수 공급실패와 반응기의 스팀 제어루프의 고장이라는 2가지의 개시원인을 확인하였다.
- 2가지의 개시원인을 예시보고서의 제3항에 입력한다.

3. 초기사고빈도

- 공정운전경험으로 이 지역에서는 15년에 한번 냉각수 공급실패의 경험을 가지고 있다.
- 평가팀은 냉각수 공급실패를 엄격하게 적용하여 10년마다 1회 적용하는 것으로 결정했다. 따라서 년간 0.1번의 사고 수치를 예시보고서의 제4항에 입력한다.
- 이렇게 해서 다른 개시원인(반응기 스팀제어 루프의 고장)을 표현하기 전까지 개시원인을 결론까지 줄곧 유지하는 것이 필요하다.

4. 방호계층설계

- 공정지역은 방폭지역으로 설계되어 있고 그 지역은 사실상 공정안전관리계획을 가지고 있다. 그 계획의 한 가지 요소는 위험지역에서 전기설비를 교체할 때의 변경관리절차이다.

- 방호계층분석팀은 변경관리절차 때문에 10이라는 인자에 의해 존재하는 점화원의 위험도는 감소한다고 평가한다.
- 따라서 0.1이라는 값을 예시보고서의 제5항에 입력한다.

5. 기본공정제어시스템

- 반응기에서의 고압은 반응기에서의 고온에 의해 동반되어 발생한다. 기본공정제어시스템은 반응기의 온도를 기준으로 반응기 쟈켓으로 투입되는 스팀량을 조절할 수 있는 제어루프를 가지고 있다.
- 기본공정제어시스템은 반응기의 온도가 설정값이상으로 상승하면 투입되는 스팀을 차단할 것이다. 고압을 예방하기 위해 스팀을 차단하는 것만으로 충분하기 때문에 기본공정제어시스템은 방호계층이다.
- 기본공정제어시스템은 매우 신뢰할 수 있는 분산제어시스템이고 생산관련 인력들은 온도제어회로의 작동을 못하게 할 수 있는 고장을 단 한 번도 경험하지 못했다.
- 따라서 방호계층분석팀은 PFDavg가 0.1이 적절하다고 결정하고, 예시보고서의 5항에 있는 기본공정제어시스템 항목에 입력한다(0.1이 기본공정제어시스템은에 대한 최소허용값).

6. 경보

- 응축기로 투입되는 냉각수 공급배관에 계전기가 설치되어 있고 그 회로는 온도제어 회로보다는 다른 기본공정제어시스템(BPCS)의 입력 및 제어기에 연결되어 있다.
- 콘덴서로 투입되는 저온 냉각수의 유량이 적을 때는 경보를 울리고 스팀을 차단하기 위해 운전자가 개입하도록 되어있다.
- 이 경보는 온도제어회로보다는 다른 기본공정제어시스템이 제어기에 위치하고 있기 때문에 방호계층으로 인정될 수 있다.
- 평가팀은 운전원이 제어실에 항상 있기 때문에 0.1 PFDavg로 하는 것에 동의하고 이 값을 예시보고서 제5항의 경보란에 입력한다.

7. 추가적인 완화대책

- 운전지역으로의 접근허용은 공정이 가동 중일 때에는 제한된다.
- 설비가 가동중지되고 Lock-out되어 있을 때만 정비가 허용된다.
- 공정안전관리계획은 모든 비운전인력은 반드시 공정출입시 등록 및 허락을

받아야 하고 공정운전원에게 통보를 하여야 한다.
- 강화된 출입제한 조치 때문에 방호계층분석팀은 공정지역에 있는 직원의 위험성은 10이라는 인자에 의해 감소된다고 평가한다.
- 따라서 0.1을 예시보고서의 6항의 추가적인 완화대책과 위험감소항에 입력한다.

8. 독립방호계층(독립방호계층)

- 반응기는 냉각수손실에 따른 온도 및 압력에 따라 생성된 가스의 체적을 적절히 다루도록 계산된 안전밸브를 장착하고 있다.
- 물질재고량과 성분을 재검토한 후에 위험감소라는 측면에서의 안전밸브의 기여도를 평가한다. 안전밸브는 FRP탑의 설계압력이하로 설정되고 운전기간동안 안전밸브로부터 이 탑을 고립시킬 수 있는 인간실수의 가능성이 없기 때문에 안전밸브는 방호계층으로 고려한다.
- 안전밸브는 1년에 1회 분리되어 시험되고 15년 동안 운전되면서 안전밸브내에서나 배관내에서의 어떠한 막힘 현상도 발생하지 않았다.
- 안전밸브는 독립방호계층기준을 만족하기 때문에 예시보고서의 제7항에 0.01의 PFDavg값을 입력한다.

9. 중간사고빈도

- <그림 1>의 제1열에 있는 항들을 서로 곱한 다음 그 값을 예시보고서의 8항의 중간사고빈도 항목에 입력한다. 이 예제에서 얻어진 답은 10^{-7}이다.

10. 안전계장시스템

- 방호계층에 의해 얻어진 완화 및 위험감소는 회사의 위험허용기준을 만족하기에 충분하지만 압력용기에 압력전송기가 설치되어 있고 기본공정제어시스템에서 경보가 가능하기 때문에 최소의 비용으로 추가적인 완화대책은 획득가능하다.
- 방호계층분석팀은 반응기 자켓 스팀공급배관에 있는 차단밸브에 연결된 솔레노이드밸브의 전원 차단을 하기 위해서 전류스위치와 계전기로 구성된 안전계장기능(SIF)을 추가하기로 결정한다.
- 이 안전계장기능은 SIL 1의 낮은 범위까지 설계되고 0.01의 PFDavg의 값을 가진다.
- 따라서 예시보고서의 안전계장기능무결수준(SIL) 하단에 입력한다.
- 완화된 사고빈도는 이제 제8항을 제9항에 곱해서 얻을 수 있으며, 그 결과(1×10^{-9})를 예시보고서의 10항에 입력한다.

11. 다음 안전계장기능(SIF)

(1) 방호계층분석팀은 이제 2번째의 개시원인(반응기 스팀 제어회로)을 고려한다. <표 3>은 제어밸브고장 빈도를 결정하는데 이용되며 0.1이 예시보고서의 4항 초기사고빈도 아래에 입력한다.

(2) 공정설계, 경보, 추가적인 완화대책, 안전계장시스템으로부터 얻어진 방호계층은 스팀제어회로의 고장이 발생하면 여전히 있을 수 있다. 실패한 유일한 방호계층은 기본공정제어시스템이다. 방호계층분석팀은 중간사고빈도(1×10^{-6})와 완화된 사고빈도(1×10^{-9})를 계산한다. 그 값을 예시보고서의 제8항과 제10항에 각각 입력한다.

(3) 위험과운전분석(HAZOP)에서 확인된 모든 이탈들이 규명될 때까지 이 분석을 계속한다.

(4) 마지막 단계는 완화된 사고빈도를 같은 위험성이 존재하는 심각한 사고 및 매우 심각한 사고에 대해 더하도록 한다.

(5) 이 보기에서, 전체과정에서 오직 하나의 영향사고가 확인되었다면 그 수는 1.1×10^{-8}이 된다. 점화확률은 공정설계(0.1)하에서, 공정지역에 사람이 있을 확률은 추가적인 완화대책(0.1)하에서 설명되기 때문에 화재로 인한 사망사고의 위험에 관한 계산은 다음과 같이 줄어든다.

- 화재로 인한 사망사고 = (모든 인화성물질의 누출의 완화된 사고빈도) × (화재로 인한 사망사고의 확률) 또는,
- 화재로 인한 사망사고의 위험도 = $(1.1 \times 10^{-8}) \times (0.5) = 5.5 \times 10^{-9}$

이 수치는 회사의 위험허용기준이하이므로 더 이상의 위험감소대책은 경제적으로 적정하지 않다고 고려되며, 이로서 방호계층분석 작업은 종료된다.

방호계층분석 결과서(예시)

#	1	2	3	4	5			6	7	8	9	10	11
					방호계층								
순서	영향 설명	강도 수준	초기 사고 원인	초기 사고 빈도	일반적인 공정 설계	기본 공정 제어 시스템	경보 등	추가적인 완화 대책, 접근 제한 등	독립 방호 계층, 추가적인 완화 대책, 다이크, 압력 방출	중간 단계의 사고 빈도	안전 계장 기능 무결 수준	완화된 사고 발생 빈도	비고
1	증류탑 파열로 인한 화재	심각	냉각수 손실	0.1	0.1	0.1	0.1	0.1	PRV 01	10^{-7}	10^{-2}	10^{-9}	고압으로 인한 증류탑 파손
2	증류탑 파열로 인한 화재	심각	스팀제어루프 고장	0.1	0.1		0.1	0.1	PRV 01	10^{-6}	10^{-2}	10^{-8}	위와 동일
N													

안전보건기술지침 개정 이력

□ 개정일 : 2023. 8. 24.

○ 개정자 : 안전보건공단 전문기술실 오상규

○ 개정사유 : 산업안전보건법 관련 법령조항 삭제

○ 주요 개정내용

- **(1. 목적)** 액산업안전보건법 제 49조의2(공정안전보고서의 제출 등), 같은 법 시행령 제 33조의 7(공정안전보고서의 내용) 및 같은 법 시행규칙 제 130조의 2(공정안전보고서 세부내용 등)" 법령 조항 삭제