KOSHA GUIDE
X - 53 - 2012

시스템 설계단계에서의 리스크 평가지침

2012. 11.

한국산업안전보건공단

안전보건기술지침의 개요

○ 작성자 : 사단법인 한국안전학회
충북대학교 안전공학과 임현교

○ 제·개정 경과

- 2012년 8월 리스크관리분야 제정위원회 심의(제정)

○ 관련규격 및 자료

- ISO 4254-1, Tractors and machinery for agriculture and forestry, 2005
- ISO/IEC Guide 37, Instructions for use of products of consumer interest, 1995
- ISO 14121-1, Safety of machinery, 2007
- ISO 12000-1, Safety of machinery, 2003
- ISO 13852, Safety of machinery, 1996
- IEC 61511-1, Functional safety, 2000
- KOSHA GUIDE X-1-2011 (리스크 관리의 용어 정의에 관한 지침)
- KOSHA GUIDE X-6-2012 (고장형태와 영향분석(FMEA)기법에 관한 지침)
- KOSHA GUIDE X-13-2012 (중소규모 사업장의 리스크평가 관련 유해위험요인 분류를 위한 기술지침)
- KOSHA GUIDE M-123-2012 (기계류의 위험성평가 지침)

○ 기술지침의 적용 및 문의

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

공표일자 : 2012년 11월 2일
제 정 자 : 한국산업안전보건공단 이사장

KOSHA GUIDE
X - 53 - 2012

시스템 설계단계에서의 리스크 평가지침

1. 목 적

이 지침은 시스템과 관련된 사고를 예방하기 위하여, 시스템의 설계 단계에서의 설계원칙 및 리스크 평가시 검토되어야 하는 기술적 사항을 제공하는 데 목적이 있다.

2. 적용범위

이 지침은 시스템 생산 및 제조 현장 중 시스템을 설계하는 현장에 적용한다.

3. 용어의 정의

(1) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

(가) “생산시스템(이하 “시스템”이라 한다)”이라 함은 여러 요소로 구성된 시스템으로서, 사용자에게 판매 후 제품생산을 위해 이용되는 산업기기 및 설비를 말한다.

(나) “수명 주기 (Life cycle)”라 함은 생산시스템의 구상단계에서 시작하여 완전히 폐기될 때까지의 안전성을 평가함에 있어서 고려되어야 하는 전체 기간(IEC 61511-1: 2003 참조)을 말한다.

(2) 그 밖에 이 지침에서 사용하는 용어의 정의는 이 지침에 특별한 규정이 있는 경우를 제외하고는 산업안전보건법, 같은 법 시행령, 같은 법 시행규칙, 산업안전보건기준에 관한 규칙 및 KOSHA GUIDE X-1-2011(리스크 관리의 용어 정의에 관한 지침)에서 정하는 바에 의한다.

4. 시스템에 요구되는 안전성

(1) 고려 대상으로 하는 시스템의 안전성의 범위는, 시스템이 개발되어 시장에 출하되고 유통되어 판매되고 최종적으로 그 시스템의 사용이 종료된 후에 폐기 처분되기까지의 수명 주기(Life cycle) 전체를 대상으로 한다.

(2) 다음과 같은 사항이 시스템의 리스크 관리에 포함된다.

(가) 설치시의 안전성

(나) 운용시의 안전성

(다) 유지보수시의 안전성

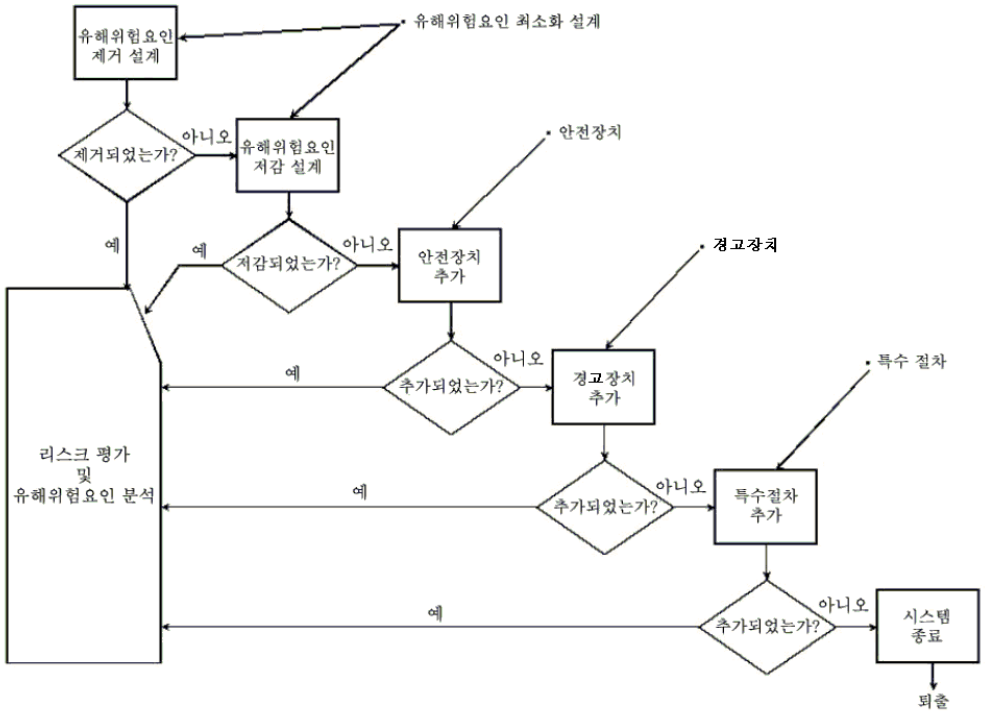
(라) 폐기시의 안전성

(마) 기타 시스템 특성에 맞는 수송시, 보관시, 판매시의 안전성

5. 시스템의 안전설계 원칙

5.1 시스템 안전을 위한 기본 원칙

(1) 시스템과 관련된 사고를 예방하기 위하여 설계자는 <그림 1>과 같은 안전설계의 절차를 반드시 순서대로 준수해야 한다.



<그림 1> 시스템 안전 우선순위 (Roland, 1983)

(가) 가능한 한 시스템의 설계를 통하여 유해위험요인을 제거하거나 저감시킨다.

(나) 제거할 수 없는 유해위험요인에 관해서는 효과적인 방호장치를 설치한다.

(다) 방호 수단의 채용에도 불구하고 남아 있는 유해위험요인에 관해서는 경보장치, 매뉴얼, 라벨, 픽토그램 등을 통하여 사용자에게 알린다.

(라) 사용자는 개인보호구를 착용하거나, 훈련이나 교육 등 관리적인 방법을 통하여 유해위험요인에 노출되는 시간을 가능한 한 단축한다.

(2) 시스템을 설계할 때에는 시스템이 시장에 출하되어 사용자의 손에 전해져 최종적으로 사용이 완료되어 폐기될 때까지 발생 가능한 유해위험요인을 예측하여 유해위험요인을 제거하고 회피해야 한다.

(3) 시스템에 내재되어 있는 모든 유해위험요인을 제거하고 회피할 수 없는 경우에는 설계를 변경하여 유해위험요인을 경감시켜야 한다.

(4) 제거하거나 경감하는 것이 불가능한 경우에도 그 시스템에 내재하고 있는 유해위험요인원에 사람이 접근하거나 접촉하여 위험한 상황에 처하지 않도록 해야 한다.

(5) 유해위험요인 회피를 위한 경고 또는 지시를 사용자 및 그 밖의 관계자에게 전달해야 한다.

6. 시스템 설계단계에서의 리스크 평가

6.1 리스크 평가의 대상

시스템의 설계단계에서의 리스크 평가는 시스템의 구상, 설계, 개발, 설치, 운용, 유지보수, 폐기 등 전 수명주기에 걸쳐서 다음과 같은 사항들을 평가의 대상으로 한다.

(1) 시스템의 구성 및 운용과 관련된 원재료, 기계, 설비, 공구 등의 하드웨어

(2) 시스템의 운용 및 유지보수에 관련된 작업방법, 작업지시, 유지보수 등의 소프트웨어

(3) 시스템의 구상에서부터 폐기의 전 과정에 관계된 작업자, 주변작업자, 관리자, 제3자 등

(4) 시스템이 노출되는 작업환경 등

6.2 평가 범위

시스템 설계 단계에서 실시하는 리스크 평가는 해당 시스템의 수명주기 전반에 걸쳐 평가 대상을 평가에 고려하여야 한다.

6.3 리스크 평가 내용

(1) 기계적 위험요인

(가) 위험점이 노출된 가동부분

(나) 위험한 표면을 지닌 부품

(다) 불안전한 운송수단 및 작업도구

(라) 불안전한 부분

(마) 넘어짐(미끄러짐, 걸림, 헛디딤)

(바) 추락

(2) 전기적 위험요인

(가) 감전

(나) 아크

(다) 정전기

(3) 물질에 의한 유해위험요인

(가) 가스

(나) 증기

(다) 에어로졸

(라) 유동액

(마) 고체

(바) 반응성 물질

(사) 방사선

(4) 생물학적 유해위험요인

(가) 미생물, 바이러스 또는 생물학적 요인에 의한 감염 리스크

(나) 유전자 변형물질 (Genetically modified organism, GMO)

(다) 알러지 및 미생물

(5) 화재 및 폭발 리스크

(가) 고체, 액체 및 가스로 인한 화재·폭발 리스크

(나) 복사열·폭발 압력

(다) 폭발물질

(6) 고열 및 한냉 유해위험요인

(가) 고열에 노출

(나) 한냉에 노출

(7) 물리학적 작용에 의한 유해위험요인

(가) 소음

(나) 초음파, 초저주파음

(다) 진동

(라) 저압 또는 고압 상태

(마) 질식

6.4 리스크 평가의 기술적 착안점

시스템의 안전성을 확보하기 위한 설계상의 기능을 평가할 때에는 다음과 같은 기술적 사항에 주목한다.

6.4.1 시스템의 보호 안전 기능

(1) 조작 정지 기능 (Operational stop function)
제품, 가공품, 공정 등에서 피해를 피하기 위하여 동작 중의 특정 부분에서 동작을 정지한다.

(2) 안전 보호 정지 기능 (Safety stop function)
기대하지 않은 운전을 방지하기 위하여 정해진 상황이 되면 곧바로 시스템을 안전한 상태(정지)로 한다. 리셋 기능과 연동시키는 경우가 일반적이다.

(3) 비상정지 기능 (Emergency stop function)
위험 상황이 되면 시스템의 기능이 긴급하게 정지하는 기능이다. 그러나, 시스템의 특성에 따라서는 긴급 정지가 오히려 상황을 더 악화시킬 수 있다는 데 주의하여야 한다.

(4) 리셋 기능 (Reset function)
시스템을 기동시키기 전에 안전 장치 등에 내장된 수동 기능에 의하여 초기 상태로 복귀시키는 기능이다.

(5) 재기동 (Restart function)
리셋 신호와의 논리합으로, 시스템의 안전이 확인되고 시스템이 동작을 개시하는 초기 상태로 설정되어 있으면 재가동을 가능케 한다.

(6) 반응 시간 (Reaction time)
시스템의 위험을 감지하여 안전 기능이 반응하여 안전 상태가 될 때까지

시간을 말한다. 유해위험요인을 검증하고부터 손상을 받기 전에 리스크를 회피하는 것이 가능할 만큼 시간이 충분하여 안전 장치는 목적을 달성한 것으로 볼 수 있다.

(7) 안전 파라미터 (Safety parameter)
미리 설정한 제한 조건을 넘은 때에 검지하여 안전장치를 기동시키는 기준 변수 값을 말한다. 위치・속도・압력・온도・유량・농도・거리・고도 등의 파라미터로 이상을 검지하는 경우가 많다.

(8) 뮤팅 (Muting)
시스템 가동 중에 있어서 당해 안전 장치의 기능을 일시적으로 휴지 상태로 하는 경우를 말한다. 뮤팅 중에도 사람에 대한 안전 기능(Human safety)은 유지되지 않으면 안 된다.

(9) 기계적 제로 상태 (Zero mechanical state)
위험 부위에 근접할 때에는 그 곳의 위험한 에너지를 제로로 한다고 하는 사고 방식이다.

6.4.2 방호장치

시스템의 구조상 위험으로부터 물리적 방호를 시행하는 장치를 말한다.

(1) 고정식 방호장치
용접, 나사 조임 등에 의하여 방호장치를 고정한 것으로, 공구를 사용하지 않고는 방호장치를 제거하는 것이 불가능하도록 설계한다.

(2) 가동식 방호장치
슬라이드 기구나 힌지 기구로 시스템에 설치된 방호장치로서, 공구 등으로 방호장치를 의식적으로 조정할 수 있다. 방호장치가 해제되었을 때, 부주의로 위험한 조작이 가능해지는 것을 방지하도록 고려한다.

(3) 조절식 방호장치
구멍이나 목표물에 맞추어 설치, 조정하면 위기를 피할 수 있도록 한 것으로서, 시스템을 조작하는 데에는 조정 위치에 고정된 상태로 한다.

6.4.3 안전장치

방호장치를 조합하거나 단독으로 시스템에 내장시켜, 시스템으로서 리스크를 저감하거나 리스크를 해제하는 장치이다.

(1) 인터록 기구
방호장치가 설정되어 있지 않는 한 시스템의 위험한 기능 조작이 불가능한 기계적 전기적인 안전 기구이다.

(2) 불능 제어 장치
시스템의 기동과 연동하는 부가적인 수동 제어 장치이다. 불능 제어가 연속 (On) 상태가 아니면 시스템이 기동하지 않는다.

(3) 수동 작동유지 (Hold-to-run) 제어 장치
작업자가 자기 손으로 구동장치를 유지하지 않는 한 시스템의 기동 운전은 불가능해지게 된다.

(4) 양수 제어
수동 작동장치 두 개를 동시에 기동시키지 않으면 시스템의 기동, 동작의 유지가 불가능하게 된다.

(5) 트립 (Trip) 장치
사람이 안전한 영역을 넘어서 위험 영역에 신체의 일부가 침입하였을 때 시스템 기능 전체 또는 기능의 일부가 정지한다.

(6) 기계적 폭주 억제 장치
쐐기, 기둥, 회전축 등 기계적 장애물을 기구부에 내장함으로써, 시스템이 임계치를 넘어 폭주 동작하는 경우를 상정하여 방어한다.

(7) 리미팅 (Limiting) 장치
공간거리, 압력제한, 전압제한, 속도 제한 등 설계적으로 제한된 조건을 넘지 않도록 예방하는 장치이다.

(8) 이동 제한 장치
이동 기구부의 이동 영역은 이동 총량을 제한된 범위로 억제한다. 이동폭은 각각의 리미터를 설정한 범위로 억제된다.

(9) 접근 방지 장치
위험영역의 접근을 본질적으로 방어하고 있지는 않지만, 함부로 접근하지 않도록 울타리 등을 설치하여 사람의 접근 가능성을 저감시킨다.

6.4.4 전기적으로 고유한 안전 대책

(1) 감전 및 에너지 위험의 보호 쉴드
사용자의 접근 가능한 범위, 사용자 접근에 대하여 방지한다.

(2) 절연 특성의 확보
내전압, 내열성, 제품에 사용되는 기간, 상정되는 환경에 의한 열화, 흡습 및 기계적 강도를 고려하여 절연물을 선택한다.

(3) 전류 제한 회로 기술의 확립
과부하에 대한 전류·전압 제한, 절연 파괴, 부식 가능부분 등에 흐르는 과전류의 제한, 에너지 차단 등의 기술을 확립한다.

(4) 접지 방법
안전하고 신뢰성이 높은 보호 접지 기술의 기준을 설정한다.

(5) 1차 전원의 분리 및 1차 회로에 있어서 과전류 방지와 접지의 보호
고장 시에 흐르는 전류의 차단, 보호장치가 동작함으로써 위험 유발을 방지한다.

(6) 안전 인터록 구비 조건의 설정
커버나 문이 붙은 경우 인터록 기능의 동작 조건을 명시하고 표시한다. 리스크의 정도에 따라 인터록 시스템이 고장 났을 때의 안전 확보 방법도 고려한다.

(7) 공간 거리, 연면 거리 확보 기준

절연 파괴 및 오염에 의한 트래킹(Tracking) 사고를 예방한다.

(8) 정전기 방전에 의한 위험보호
제품의 설치, 사용환경에 있어서 정전기 방전에 의해 발생하는 제품의 위험을 방지한다.

(9) 전자파 적합성 (EMC)에 대한 고려
아크 또는 스파크, 무선기 및 휴대 전화의 전파, 기타 전기장치로부터 방사되는 전자파로부터 보호되어야 하며, 외부로 과다한 전자파가 방사되지 않도록 한다.

(10) 온도 상승치의 제한
제품 표면, 내부의 온도의 상승을 제한하여, 보온·난방 기구에 의한 저온 화상을 방지한다.

6.4.5 화학 제품의 고유한 안전성

제품에 따라 매우 다양하고 검토하여야 할 항목이 많다. 대표적인 것들을 나열하면 다음과 같다.

(1) 내부식성
화학물질에 의한 제품의 부식, 위험한 화학 물질의 누출을 방지한다.

(2) 인체에 직접 흡입되는 제품의 불순물에 의한 건강 장해 예방

(3) 인체가 노출되는 화학 제품에 의한 건강 장해 예방

(4) 화학적 해리에 의한 영향

(5) 화학적 치환, 산화에 의한 영향 등.

6.5 설계단계에서의 리스크 평가 요령

(1) 신기술의 리스크를 평가할 수 있는 많은 양의 자료가 축적되므로, 이를 잘

정리, 보관하도록 한다.

(2) 출력물로서의 제품 또는 시스템의 설계가 이루어지는 때이므로, 구체적인 자료를 이용한 리스크 평가나 신뢰성 평가가 가능해지는 때이다.

(3) 일반적인 평가기법으로는 위험요인과 운전분석(Hazard and operability studies, HAZOP) 기법이나 고장형태와 영향분석(Failure modes and effects analysis, FMEA) 기법 등이 적절하다. <부록 1> 참조.

(4) 설계가 진행됨에 따라 자료도 풍부해지고, 설계안도 구체화되므로, 리스크 평가도 이에 따라 몇 차례고 반복되어 허용 불가능한 리스크를 가진 부분이 남아 있도록 해서는 안 된다.

(5) 이 단계에서 얻어진 리스크 평가 결과는 대량생산으로의 지속 여부를 결정짓는 중요한 자료이므로, 사소해 보이는 유해위험요인이라도 소홀히 취급해서는 안 된다.

<부록 1>

적용사례

고장형태와 영향분석 (예시)

시스템 염화암모늄플랜트 | 수정안 Version 2.2
서브시스템 염산수용액공급시스템 | 분석자 홍길동
부품번호 B26230-A100 | 분석일자 '10/02/27
설계 책임자 박문수 | 수정일자 '12/09/16

고장형태와 영향분석
(Failure Modes & Effects Analysis)

기기	기기정보	고장형태	시스템기능/안전에 미치는 영향	영향도	안전 대책	담당	종료(예정)
유량비 제어밸브 CPS-V100	상시 운전 재질 염산 사양	1.a 개방 고장	1. 반응기에 염산수용액이 과잉 유입되어, 규격 외의 제품이 생산됨 (고염산농도)	보통	P1. 염산수용액 라인에 유량계 설치 염화암모늄 제품 분석	공정팀	' 10.12.11
			2. 공급탱크가 비어, 공급 펌프가 손상됨	보통	TC21.공급탱크에 액면계 설치	공정팀	' 11.01.16
			3. 반응기 또는 염화암모늄 탱크의 액면이 상승하여 넘쳐 흐름	보통	N100.운전원의 염화암모늄 탱크 감시	공정팀	-
			4. 암모니아 수용액 유량이 점차 증가하여 반응기의 습도, 압력이 상승하고 파괴됨	높음	R72. 반응기에 안전밸브 설치	공정팀	'12.10.30
		1.b 폐쇄 고장	1. 유량계 고장에 의한 전면 폐쇄의 경우, 염산수용액의 공급 정지와 아울러 암모니아 수용액의 공급도 정지하여, 반응정지에 이름	보통	P1. 염산수용액 라인에 유량계 설치	공정팀	' 10.12.11
			2. 기계적 고장에 의한 전면 폐쇄의 경우, 암모니아 수용액의 공급은 계속되므로, 염화암모늄 탱크에 암모니아 수용액이 유입되어 건물 내에 암모니아 증기가 발생되어, 중독될 위험이 있음	높음	Z83-9. 건물 내에 암모니아 검지경보기 설치	기계/건설팀	미정
		1.c 고착	1. 전면개방 또는 전면폐쇄로 고착된 경우에는 위 1.a 또는 1.b와 같음	-	QA.Proc 20-6 유량비 제어밸브의 정기 점검 및 보수	보전팀	-
			2. 평상시처럼 열려 있는 상태에서 고착된 경우에는 염산수용액이 과잉 유입되어 크게 영향 없음	낮음	QA.Proc 20-6 유량비 제어밸브의 정기 점검 및 보수	-	-
		1.d 외부 누출	1. 건물 내에 소량의 염산 증기 발생, 위험	보통	QA.Proc 20-6 유량비 제어밸브의 정기 점검 및 보수 제어밸브 재질은 산성 사양	-	-
염산수용액 공급 정지	상시 운전	1.a 전면 정지	1. 암모니아 수용액 유량이 점차 증가하여 반응기의 습도, 압력이 상승하고 파괴됨	높음	R72. 반응기에 안전밸브 설치	공정팀	'12.10.30
		생략	생략	생략	생략	생략	