시스템 안전 분석기법 활용방안

충주대학교 안전공학과
김 병 석 교수

1. 서론

사업장에서 안전활동이 불충분해 사고가 일어나면 근로자의 상해뿐만 아니라 장치, 개발, 또는 제조 중인 제품에 피해를 주어 예상된 시스템 안전프로그램 수행에 지장을 초래한다. 즉 사고가 없어도 불안전한 환경에서는 불량제품 또는 불량부품 등이 제작될 가능성이 많아지고 시스템 안전설계 실현이 어렵다. 그러므로 시스템에 안전성이 없으면 제조과정에서도 사고가 일어날 위험성이 높고 생산성이 떨어진다는 것은 분명한 사실이다.

현재와 미래의 글로벌 스탠다드에서의 기업들은 과거 발생된 과거 데이터에만 의존하는 것보다는 여러 위험분석기법들을 활용하여 미래에 발생되거나 예상될 수 있는 위험을 식별하여 생산성 향상에 저해가 되는 위험성을 미리 제거하여 안전성 확보측면에 더욱더 관심을 가져야 될 것이다.

시스템안전 프로그램은 신규시설의 도입 시에나 유지측면에서 설치, 검사, 시운전, 작업, 보전, 교육, 훈련 등의 단계에서 생산성의 원활화와 근로자의 안전확보 면에서 사용자의 협조아래 시스템 안전프로그램을 작성 실행하게 된다. 미국의 시스템안전은 초기에는 미 국방성 무기시스템이나 제품의 안전을 위해 개발되었지만 현재는 시설, 제조 등 모든 산업에 해당되는 안전을 목적으로 한 총괄적인 시스템 안전프로그램으로 시도되고 있다.

우리 나라에서도 선진국과 같이 사업장의 근원적인 안전성 확보를 하기 위하여 각 사업장별로 안전관련 팀을 구성하여 제품이나 공장설계 시부터 총체적 근원적 안전관리 시스템을 구현하기 위하여 함께 연구하여야 될 것이다.

본 논문에서는 선진국 등에서 시행되는 과학적 위험관리 기법 등을 분석하여 우리나라 사업장에 알맞은 안전관리 시스템개발에 적용하기 위한 자료로 활용하고자 한다. 따라서 국내 위험관리와 외국에서 시행되는 과학적 위험관리를 비교하여 분석하고 국내에 맞는 위험관리 시스템 기법을 적용하기 위한 기초자료로 활용하고자 한다.

2. 조사방법

본 논문의 연구방법은 국내와 국외로 구분하였

으며, 국내는 산업안전보건법을 기본으로 하는 위험관리 방법 등을 검토하였으며, 외국은 미국의 총체적 안전관리 시스템과 연관된 시스템 2000의 위험관리방법을 비교하였다.

또한 외국 시스템안전 프로그램개발에서 각 단계별 위험분석 기법의 특징은 기존 국내·외 학자들의 저서와 논문을 조사 분석하였으며 운영과 실태 면에서는 시스템안전공학을 기초로 하여 확인을 하였다.

3. 시스템안전 연구영역 및 프로그램 분석

가. 시스템안전의 연구영역

시스템에서 안전성을 확보하기 위해서는 작업라인의 책임 하에서 효율적이고 비용이 절감된 생산시스템이어야 하며, 가능한 설비나 제품의 제조공정 중에 최적의 안전설계를 하여야 한다. 안전장치, 경보장치, 작업방법, 훈련통제 등은 그 후 순차적으로 고려되어야 한다.

그러나, 현재 우리 나라에서는 전자보다 후자의 작업방법, 훈련 등을 우선적으로 적용하는 경향이 있다. 이것은 시스템안전 기술부족의 현상이라고 판단된다. 아래의 〈표 1〉은 우리 나라 법령에 준한 안전관리와 시스템안전의 비교분석을 나타낸 것이다.

나. 시스템안전 프로그램 개발 방법

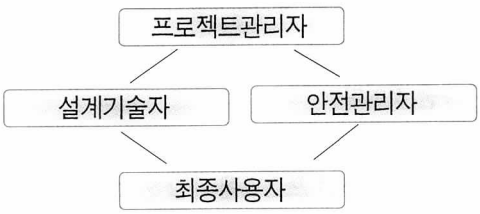
선진국에서는 특히 1980년 중반부터 시설, 건설물에 적용시키기 위한 총체적 시스템으로 공학자, 설계자, 안전기사, 사용자 등으로 SSWG(System Safety Working Groups) 팀을 구성하여 〈그림 1〉 에서와 같이 구성하여 진행하고 있다.

이 팀의 구성을 보면 각 파트별로 업무영역이 다르게 느껴지나 실질적으로는 총체적 프로그램 개발이 하나로 통합되기 때문에 각각 서로의 밀접한 연관관계를 가지고 진행되는 것을 볼 수 있다. 즉 각 부분별 업무에서 하나의 에러가 발생되면 안전관리의 총체적인 문제가 발생되기 때문에 시스템 안전관리자들은 전체의 위험시스템을 체계적으로 하기 위한 분석 기법 등을 활용, 능숙하게 분석하여야 하는 것은 당연한 일이다.

그러므로 우리 나라에서도 생산과 안전이 연관된 SSWG의 팀을 구성하여 원활한 안전관리 문제의 해결을 위한 흐름을 유지하는 것이 무엇보다 중요하다고 본다.

〈표 1〉 법령에 준한 안전관리와 시스템안전의 비교

분 류	비 교 내 용
법령, 법규, 규정, 표준 등 (산업안전)	1) 100% 법규 등을 준수하더라도 단지 최소한의 안전성확보 2) 급격한 변화기술에 미흡
시스템안전	1) 위험수준을 줄일 수 있는 최고수준의 안전장치 2) 체계적 위험분석, 총체적 시스템의 최적 안전 중점, 생산성과 연결설계



〈그림 1〉 미국의 시스템안전 수행 작업그룹 (SSWG)

다. 시스템안전 프로그램의 개발 방법에서의 위험분석

미국에서는 위험평가와 위험관리가 특징적이다.

미국은 물리적인 제품, 설비 등의 안전관리와 인적원인, 근로자 안전을 별도로 적용하여, 〈그림 1〉와 같이 총체적, 안전시스템에서 총괄하는 형태로 관리되어지고 있다. 특히 위험범위를 〈표 2〉과 같이 자주발생, 보통발생, 가끔발생 등으로 구분, 위험관리 우선 순위를 설정하고, 〈표 3〉과 같이 위험 중요도를 구분하였다. 또한 위험관리를 위한 여러 형태의 위험분석기법들은 사업장에 맞는 실질적 생산성 향상을 기여하는데 큰 역할을 하고 있다.

〈표 2〉 위험 가능성

구 분		발 생 현 황	
		개별항목	전체항목(시스템)
자주 발생	A	때때로 일어날 듯 함	연속적 경험
보통 발생	B	한 항목의 수명 중 수회 일어남	때때로 일어남
가끔 발생	C	한 항목의 수명 중 수회 일어남	수회 일어남
거의 발생 하지 않음	D	그리 일어날 것 같지 않음	일어날 것 같지는 않으나 존재 가능성
극히 발생 하지 않음	E	발생확률 0에 가까움	위험을 경험하지 않은 것으로 가정함
전혀 발생 하지 않음	F	물리적 발생 불가능	물리적 발생 불가능

4. 시스템안전 프로그램의 수명주기와 위험분석 기법

가. 시스템안전 프로그램의 수명주기(Life cycle)

시스템 수명주기(System life cycle)를 5단계로 구분하면 일반적으로 〈표 4〉에서 보는 바와 같이 구상단계(Concept), 정의단계[혹은 사양결정단계(Definition)], 개발단계(Develop - ment), 생산단계(Production), 운전단계(Deployment)로 나누어지고 하나 더 추가하면 마지막 단계인 폐기단계(Disposal)가 있다. 이들 각 단계들은 시스템을 전개하기 위해 만들어진 용어로서 서로 밀접한 관계가 있다.

나. 시스템안전 프로그램의 수명주기별 분석기법 적용

〈표 3〉 위험 중요도

분 류	범주	해당 재난
파국(catastrophic)	Ⅰ	사망 또는 시스템 상실
중대재해(critical)	Ⅱ	중상, 직업병 또는 중요 시스템 손상
경미재해(marginal)	Ⅲ	경상, 경미한 직업병 또는 시스템 가벼운 손상
무시재해(negligible)	Ⅳ	사소한 상처, 직업병 또는 시스템 손상

〈표 4〉 시스템 프로그램 단계별 용어

단 계	명 칭
1 단 계 구상	(Concept)
2 단 계 정의	(Definition)
3 단 계 개발	(Development)
4 단 계 생산	(Production)
5 단 계 운전	(Deployment)

〈표 4〉에서와 같이 수명주기 5단계별 위험분석법을 적용할 수 있다.

(1) 제 1 단계(구상단계, 사양결정단계)

제 1 단계에 이론은 구상단계와 사양결정단계가 있다. 구상단계는 설비 및 제품사용에 연관된 위험요인을 발견 · 검토한다. 사양결정단계는 위 위험요인 검토결과 적절한 제어조치의 사양을 정한다.(안전도 및 신뢰도 포함) 이 단계에서 사용되는 분석법에는 PHA (Preliminary Hazard Analysis), Risk Analysis, SSPP(System Safety Program Plan)등이 있다. PHA는 특정사항에 연관된 위험확인 분석용으로 사용(초기위험 분석)한다. Risk Analysis는 전체수준의 설계기준개발 위험관리로 이용한다. SSPP 최고 경영자와 구매자가 안전시스템 개발을 위해 계약을 체결한다.

(2) 제 2 단계(설계단계)

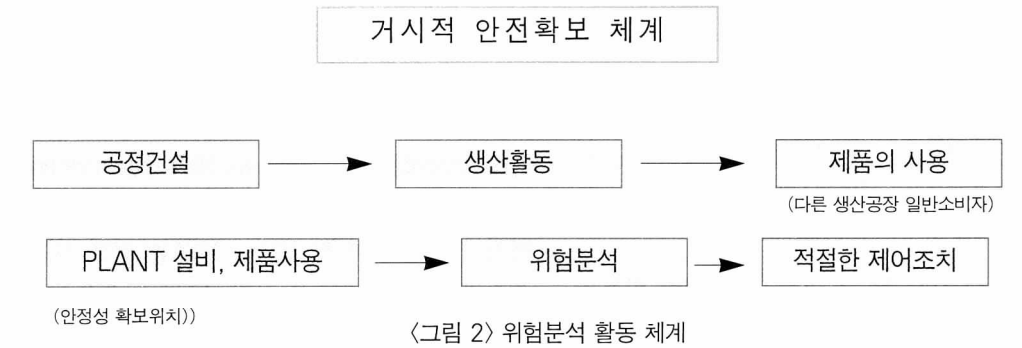
제 2 단계에 설계단계이다. 이 단계는 시스템 안전 프로그램의 중점이 되는 단계(안전성과 신뢰성 목표)이다. 그리고, 기본설계와 세부설계로 나눈다. 시스템 과정에 맞는 구조와 제어방식을 선택(구조적 안전 : 안전장치, 방호장치 : 경보장치)한다. 설계 시 리스크, 비용, 인간공학, 운영과 보존적합성 등을 적용 검토한다. 설계 제공하기 위해 서브시스템, 서브어셈블리. 어셈블리가 명확히 정의된다. 적용되는 분석기법에는 SSHA(Subsystem Hazard Analysis), FHA(Failure Hazard Analysis) · FTA(Fault Tree Analysis), Risk Analysis, Risk Examination 등이 있다. SSHA는 PHA를 새롭게 한다.(조치까지 포함되기 때문) FHA · FTA는 알고 있는 특정위험과 잠재위험을 시험, FHA 구성요소나 사건이 SSHA, SHA의 안전에 영향을 주는 결정적 요인이다.

Risk Analysis는 예비단계에서의 다른 위험을 평가(분석)하는데 도움이 된다. Risk Examination는 최종설계를 선택할 수 있는 핵심요소이다. 그리고 기타 안전분석기법은 안전장치, 안전설계의 선택된 설계형태를 보증하기 위한 테스트 모델로 활용한다.

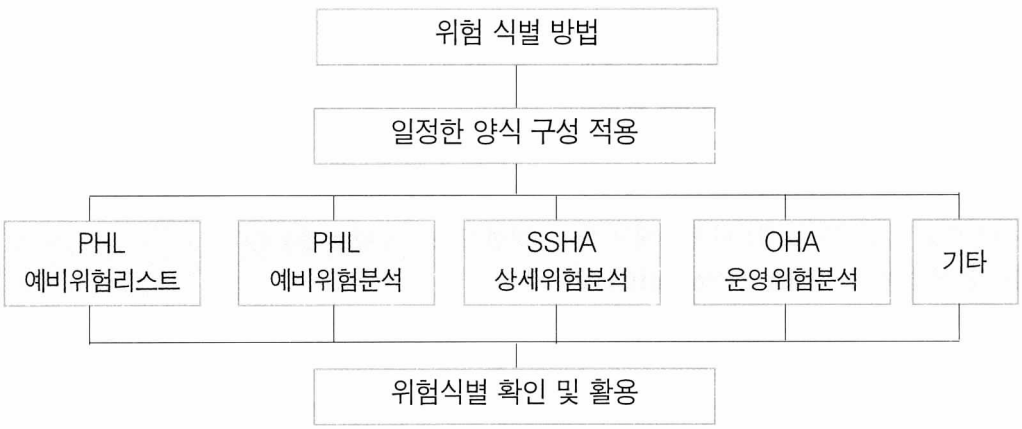
(3) 제 3 단계(개발 및 제작단계)

제 3 단계는 안전 설계된 것을 개발 및 제작한다. 개발단계에서 완벽테스트 실시하고, 설계 수용가능 여부결정 한 후 제작 결정한다. 실제로 설비운전, 설비사용조건 등을 구체적으로 검토한다. 작업표준측면에서는 작업을 단위동작으로 분석하는 것이 필요하다. 보전의 방식에서는 어느 정도 주기로 어느 곳은 어떻게 정비할 것인가를 고려 해야한다. 안전점검측면에서는 점검항목별로 점검의 주기, 방법, 점검시의 착안점, 점검결과 판정 기준 등을 정한다. 안전교육 실시 단계에서는 시스템 구매자에게 공급하여 적절한 위험제어를 교육한다.

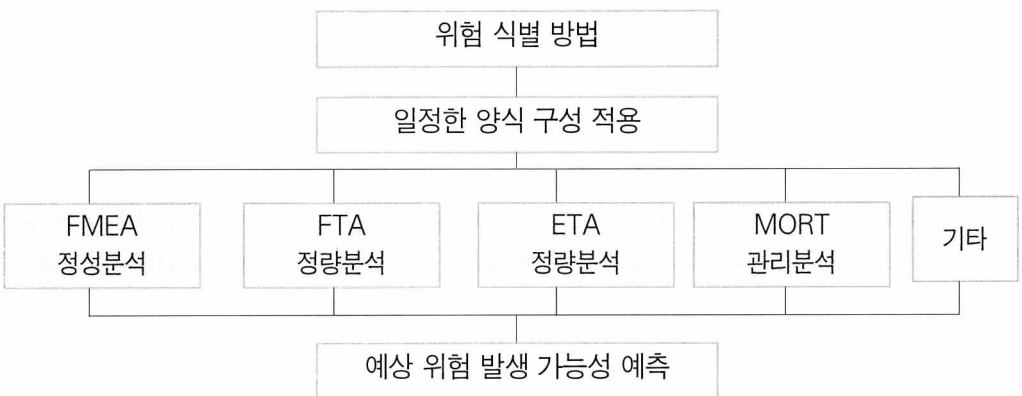
이 단계의 분석법에는 FMEA(Failure Modes & Effect Analysis), FTA, OSA(Operation



〈그림 2〉 위험분석 활동 체계



〈그림 3〉 위험식별 분석법



〈그림 4〉 위험식별 확인방법

Safety Analysis), OHA(Operating Hazard Analysis) 등이 있다. FMEA는 위험스런 고장형태를 명확하게 식별(신뢰성)한다. FTA, FHA는 FMEA의 정보로 이용된다. OSA는 제조시험을 분석한다. OHA는 PHA, SSHA, SHA를 운영위험분석으로 활용과 운영지원 위험 분석을 한다.

(4) 제 4 단계(운전단계)

시운전함에 있어 작업표준, 안전점검기준에 의하여 운전, 보전, 점검을 실시하고, 그 다음으로 안전성, 신뢰성 확보를 위해 평가한다. 이상 발견시, 과거의 재해사례, 개선사례 등 많은 자료를 활용하여 역으로 점검한다.

시스템안전분석은 〈그림 2〉과 같이 시스템 또는 설비에 관한 모든 사고를 확인하고 도입설치 및 설계 제조과정을 통하여 이들의 사고를 최소화하고 제어하는 시스템공학의 한 분야이다.

다. 시스템 안전 프로그램의 위험 식별 · 확인 분석법

새로운 형태의 위험은 식별하기 위하여 〈그림 3〉과 같이 PHL(Preliminary Hazard List), PHA, SSHA, OHA 등 일정한 양식을 활용하였으며, 식별된 위험을 더욱 정확히 정성적, 정량적으로 평가하기 위하여 〈그림 4〉와 같이 FMEA, FTA, ETA(Event Tree Analysis), MORT(Management Oversight and Risk Tree) 등 여러 형태의 기법들을 활용 사업장에 위험에 대한 문제점을 분석하였다.

5. 결론

미국 등 선진외국의 시스템안전은 우리 나라 안전관리와 분명히 차별화가 되어 있고, 특히 우리나라 안전관리가 법률주의적 안전보건법규에 의한 최소한의 안전성 확보라는 측면을 중요시하지만 여기에서 시스템안전은 실질적 최고수준의 안전성 확보라는 점에서 알 수 있다. 시스템안전을 특징적으로 관찰하면 다음과 같이 차별화 된다.

가. 시스템안전은 효율적이고 비용 절감된 생산시스템을 설계하기 위하여 제품이나 공장설계 시부터 제품생산까지 위험요인을 분석 적용하도록 하였다.

나. 보다 더 나은 안전성확보를 달성하기 위하여 법률적인 최소한의 안전성 확보 보다 실질적 최고수준의 안전시스템 구현에 목적을 두었다.

다. 시스템안전 프로그램을 실행하기 위하여 MIL-STD-882, NHB 1700(V3) 등 일정한 규격의 양식을 활용하여 위험성평가, 위험성배경, 위험범위 등을 설정하였다.

라. 시설 및 건설물의 안전관리를 위하여 공학자, 설계기술자, 안전관리자 및 최종 사용자 등 SSWG 팀을 구성하여 실질적 문제점을 분석하여 생산현장에 적용하였다.

각 사업장에 적합한 시스템 안전성 확보를 위해서는 현재 근원적이고 체계적인 위험분석과 최고수준의 안전설계를 기본으로 하는 시스템 안전 프로그램이 개발되어야 한다. 현재와 미래의 급격한 변화기술에서는 재해 발생이 더욱더 증가 할 수밖에 없다. 왜냐하면 급격한 변화 기술에 근로자가 항시 대응할 수 없기 때문이다. 따라서 새로운 기법을 활용하여 미리 위험을 예측하고 최적 안전 시스템 설계를 할 수 있도록 하여야 한다.