시스템 안전 (System Safety) 기법

朴 武 一
우리 협회 교수
건설안전기술사

1. 시스템 안전의 개요

시스템 안전이란 말은 1960년대부터 항공기, 미사일, 원자력 이용 및 우주개발 등의 복잡한 시스템에 있어 사고 예방을 위해 개발되었다. 즉 복잡한 시스템에 있어서의 잠재위험(Hazard identification)과 잠재위험억제(Hazard control)를 위한 기법의 필요성으로 개발되었고 산업재해 예방에도 활용되고 있다. 따라서 재해(Accident)과 잠재위험(Hazard)의 관계를 살펴볼 필요가 있는데 시스템 안전에서는 재해와 잠재위험을 분명하게 구분한다. 재해란 인적·물적 손실이 발생한 일(Event)을 말하고 잠재위험은 인적·물적 손실을 일으킬 수 있는 잠재적인 상태나 행동을 말한다. 즉 폭발은 재해이고, 압력용기의 균열을 잠재위험이라 할 수 있다. 따라서 시스템 안전에서는 이것을 분명히 구분하고 있다.

시스템 안전은 달성하려면 시스템의 계획, 설계, 제조 및 운용의 전단계에 걸쳐 시스템의 안전관리 및 안전공학을 정확히 적용시켜야 하며

(1) 시스템 안전관리는

① 시스템 안전사항의 인식 ② 안전활동 계획, 조직 및 관리 ③ 다른 시스템과의 조정 ④ 시스템 안전 계획(프로그램)의 해석, 검토 및 평가 등을 수행하는 분야이고

(2) 시스템 안전공학이란

과학적, 공학적 원리를 적용하여 시스템내의 잠재위험을 인식하고 예방 또는 통제에 필요한 조치를 하는 분야로서 ① 공학적 설계 ② 안전해석의 원리 및 기법을 기초로 하고 있다.

2. 시스템 안전원리

(1) 재해의 형태(Types of Accident)의 명확화

시스템의 잠재위험 인식은 먼저 시스템에서 발생할 수 있는 재해의 형태를 분류 목록화하는 것이다. 재해의 형태는 크게 "에너지 변형형"과 "에너지 부족형"으로 분류된다.

안정되고 잘 관리된 에너지라 하더라도 그것이 재해를 일으키는 방향으로 변형되었을 경우, 즉 자동차용 휘발유는 주행을 하기 위한 운동에너지로 변형되나, 충돌 등으로 화재가 되는 열에너지로 변형될 수 있다.

에너지 부족은 중요한 기능의 수행을 위한 에너지의 부족으로 재해를 발생시키는 것으로 어린이가 폐쇄된 냉장고속에서 산소의 결핍으로

질식하는 것과 같이 에너지의 부족이 직접원인으로 되는 것, 비행중의 항공기가 연료 부족으로 비행기의 추락재해를 일으키는 간접원인으로 되는 것 등이 있다.

(2) 에너지 변형 메커니즘(Energe Sources and Transformation Mechanism)

에너지 변형에 의한 재해는 에너지 변형기구와 결부되어 발생하므로 에너지원과 메커니즘(기구) 모두를 취급하여야 한다.

1) 에너지원

① 고에너지환경 : 천둥번개, 강풍, 용광로열, 소음, 진동 등

② 고에너지 구성요소 : 기계적, 전기적, 공압적 및 유압적인 요소 등

③ 저에너지 및 외형적 요소 : 약물중독, 기구의 흠집, 물질을 옷에 흘리는 것 등

2) 에너지 변형기구

① 불안전한 상태 : 마루바닥의 기름은 보행자의 위치 에너지를 변형시켜 전도시키는 불안전한 상태

② 불안전한 행동 : 유류탱크 속을 보려고 라이터 불을 켜는 것은 폭발재해를 일으키는 불안전한 행동이다.

실제로 많은 재해는 대단히 복잡한 에너지 변형기구로 되는 불안전상태와 행동의 연쇄와 구성을 포함하고 있어 시스템 안전의 주요과제는 그와 같은 연쇄나 구성을 지적하고 예방하기 위한 수단을 평가하는 것이다.

(3) 에너지 부족의 메커니즘(Energy Needs and Deficiency Mechanism)

에너지 부족형 사고는 안전에 필수적 기능을 수행하기 위한 어떤 형태의 에너지에 대한 필요와 충분치 못한 가용 에너지 발생이 둘 다 있다.

만약 공기가 질소가스로 대치된 밀폐장소에 사람이 들어가 사망했다면 생리학적 에너지 부족형 사고가 발생했다는 것이 틀림없다. 반면 사람이 밀폐장소로 들어갔으나 구조되어 아무런 상해가 일어나지 않았다면 '사고가 있었다'고 할 수 있고 후자는 '실수'였다고 한다.

즉 자동차의 유압 브레이크가 고장난 경우 재해의 유무와 관계없이 안전상 중요한 브레이크 기능이 상실하고 "바람직스럽지 못한 사상이 발생했다"라고 말한다.

재해발생과정의 불안전상태나 행동의 연쇄와 구성속에서, 에너지 부족에 의한 바람직스럽지 못한 사상의 발생은 재해발생의 빈도나 강도에 영향을 미치는 불안전상태를 만들어낸다. 따라서 사고예방을 위해서는 시스템 안전적인 "바람직스럽지 못한 사상(Event)의 발생"의 검토가 실시되어야 하는 것이다.

(4) 안전분석시기

사고예방을 위한 안전분석은 언제부터 실시하여야 하는가하는 관점도 중요하다 산업안전에서는 용접작업이나 크레인 인양작업 등에서는 단독작업이나 단계분석을 하여 왔지만 시스템 안전에서는 시스템이나 작업의 계획단계에서부터 최종단계까지를 문제로 한다.

따라서 1) 언제 분석이 행해지는가 2) 재해나 바람직스럽지 못한 사상이 언제 발생하는가가 중요하게 된다. 언제 재해가 발생하는가를 문제로 삼는 시스템 안전에서는 시험, 생산, 운반, 설치, 조업 및 폐기의 기간에 걸쳐 적용한다. 그러나 경우에 따라 항공기의 이착륙시와 같은 특히 위험한 활동에 중점을 둘 때도 있다.

3. 시스템 안전 분석기법

시스템 안전분석의 목적은

① 단독 또는 조합하여 사고나 원치 않는 사상(Event)을 야기시킬 수 있는 위험을 분명히 함

② 위험제어의 적합성을 평가하기 위함

③ 발생한 사고의 재구성을 위함

시스템 안전에 있어서 '위험'이란 용어는 산업안전에 있어서 '불안전한 상태'와 '불안전한 행동'이란 용어와 같이 물리적 상황과 인간행동을 나타낸다.

(1) 분석대상이 단순한 경우

분석대상이 극소의 잠재위험만 내포되어 있는 경우의 분석은 안전점검 리스트를 참고로 하는 정도로도 충분하다. 이런 경우의 점검 리스트는 다음과 같다.

1) 재해 형태별 점검 리스트
2) 잠재적 위험 에너지원의 점검 리스트
3) 에너지 변형기구의 점검 리스트
4) 중요 안전기능(필요 에너지) 점검 리스트
5) 에너지 결손기구의 점검 리스트

(2) 분석대상이 복잡한 연쇄나 구성된 것

분석대상이 복잡한 연쇄나 구성을 갖는 경우에는 잠재위험을 찾아내기가 무척 어렵다. 그러므로 어떤 절차와 방법이 필요하게 되는 바 이를 위하여 잠재위험 확인분석과 잠재위험 억제평가분석을 하게 된다. 이 두가지 방법은 같이 실시하지만 그 분석과정은 서로 다르다.

새로운 시스템, 조작방식 등을 개발할 때는 잠재위험의 확인을 명확하게 하기 위하여 잠재위험 억제법의 평가에서 분리시켜 실시하는 것이 원칙이다. 이유는 잠재위험이 확인되고 나서 재해강도와 발생확률을 저하시키기 위한 가능한 방법을 준비하는 데 충분한 시간을 주어야 하기 때문이다.

1) 잠재위험 확인분석방법(Hazard Identification Analysis Methods)

잠재위험을 확인하는 기본적인 사고방법은

① 연역적(바람직스럽지 못한 사상의 리스트에 의함) 방법

② 물적인 고장형태에 대한 귀납적 방법

③ 인간 과실형태에 대한 귀납적 방법이 있다.

이들의 일반적 명칭은

① 재해와 바람직스럽지 못한 사상의 원인 분석

② 물적 고장형태와 안전영향 분석

③ 인간의 과실형태와 안전영향 분석이라고도 한다.

위의 ② ③은 물적 고장과 인적인 과오 양쪽 영향을 동시에 생각할 때이고 ①은 FTA(Fault Tree Analysis) 도해를 사용 분석한다

2) 잠재위험 억제평가분석(Hazard Control Evaluation Analysis)

잠재위험이 적거나 단순한 경우 모든 점검리스트의 항목이 설계나 절차서에 받아들여졌는가를 확인하는 것만으로 평가할 수 있다. 이 경우 점검 리스트를 사용할 때에는 "잠재억제의 우선순위"는 뒤에 실시한다.

반대로 복잡한 경우에는, 시스템적 잠재위험의 확인으로 행해진 것과 같은 3개형의 분석, 즉 "FTA"또는 "안전분석"을 되풀이할 필요가 있다. 후자는 재해에 관계될 가능성이 있는 불안전 상태나 행동을 판정하여 설계나 절차서의 "지침"으로 하기 위하여 실시하고, 전자는 만들어진 설계나 절차서가 판정하고 있는 잠재위험의 억제가 효과적으로 이루어지는가를 "평가"하기 위함이다.

"평가"분석은 승인된 설계도와, 그것에 관련한 절차서의 기본에 대해서 실시한다. "지침"의 분석은 발생될 수 있는 재해의 발생확률의 대략

적인 개산(槪算)을 포함하는 경우도 있다. 간단한 평가분석에서는 "잠재위험을 억제하는 모든 대책이 취해졌는가"에 대한 답은 한계가 있다. 그러나 FTA를 사용해서 재해발생확률의 정량적 예측이 될 수 있는 경우 이 질문에 충분히 답이 가능할 것이다.

4. 시스템 안전기법의 종류

시스템 안전기법을 소개하면 다음과 같다.

(1) 세이프티 어세스먼트(Safety assessment:안전성 평가)

설비의 전공정에 걸친 안전성의 사전평가 행위를 말하며 안전성 평가는 다음의 6단계에 의하여 실시된다.

1) 관계자료의 정비 검토(1단계)
2) 정성적 평가(2단계)
3) 정량적 평가(3단계)
4) 안전대책(4단계)
5) 재해 정보에 의한 재평가(5단계)
6) FTA에 의한 재평가(6단계)

(2) 리스크 어세스먼트(Risk assessment:위험성 평가)

리스크 어세스먼트는 리스크 메니지먼트(risk management:위험 관리)와 동의어로서 산업안전에 속하는 위험관리는 바로 안전성 평가가 된다.

위험성 평가의 순서는 다음과 같다.

1) 위험성의 검출과 확인
2) 위험성 측정과 분석 평가
3) 위험성 처리(위험의 제거 내지 극소화)
4) 위험성 처리방법의 선택
5) 계속적인 위험성 감시

(3) 위험성 강도의 범주(category)

1) Category Ⅰ : 파국적(catastrophic) (사망 및 중상 또는 시스템의 상실을 일으킨다)

2) Category Ⅱ : 위기적(critical) (상해 및 중한 직업병 또는 중요 시스템의 손상을 일으킨다)

3) Category Ⅲ : 한계적(marginal) (상해 또는 주요 시스템의 손상을 일으키지 않고 배제나 억제할 수 있다)

4) Category Ⅳ : 무시(negligible) (상해 또는 시스템의 손상에는 이르지 않는다)

(4) 시스템 안전(system safety)에서의 사실의 발견기법

- FTA(Fault Tree Analysis)
- ETA(Event Tree Analysis)
- FMEA(Failure Mode and Effect Analysis)
- FMECA(Failure Mode Effect and Criticality Analysis)
- THERP(Technique for Human Error Rate Prediction)
- OS(Operability Study)
- MORT(Management Oversight and Risk Tree)

이상 소개한 기법들이 현재 널리 이용되고 있는 기법들이다.