KOSHA GUIDE
Z - 29 - 2022

사고분석에 관한 지침

2022. 12.

한국산업안전보건공단

안전보건기술지침의 개요

○ 작성자 : 한국안전문화진흥원

○ 제·개정 경과

- 2022년 12월 리스크관리분야 표준제정위원회(제정)

○ 관련규격 및 자료

- Safety-I and Safety-II: The past and future of safety management: 2014, Ashgate Publishing, Ltd.
- Safety-II in practice: Developing the resilience potentials: 2017, Taylor & Francis
- Systems thinking for safety: Ten principles A white paper: 2014, EUROCONTROL
- Accident and operational safety analysis Volume 1: 2012, Department of Energy

○ 기술지침의 적용 및 문의

- 이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈 페이지 안전보건기술지침 소관 분야별 문의처 안내를 참고하시기 바랍니다.
- 동 지침 내에서 인용된 관련규격 및 자료 등에 관하여 최근 개정 본이 있을 경우 해당 최근 개정 본을 참고하시기 바랍니다.

공표일자 : 2022년 12월 31일
제 정 자 : 한국산업안전보건공단 이사장

KOSHA GUIDE
Z - 29 - 2022

사고분석에 관한 지침

1. 목 적

기술 진보로 산업시스템이 대형화, 복잡화, 지능화, 집적화, 고위험화되어가면서 기술적 오류에 의한 사고뿐 아니라 인적오류와 관련된 사고도 빈번하다. 특히, 인적오류를 포함하는 복합사고의 경우 시스템적 논리를 바탕으로 사고의 발생 과정과 원인을 다각적으로 접근할 필요성이 있어 새로운 기법들이 개발되고 있다. 본 지침서는 이러한 복합사고와 관련된 개념과 분석 기법을 안내하는 것을 기본 목적으로 한다.

2. 적용범위

이 지침은 민간기업 및 공기관의 안전관리 감독자 또는 실무자가 인적오류에 따른 안전 사고분석 이해와 분석에 적용한다.

3. 용어의 정의

3.1 사고분석: 사고분석은 시스템 안전 향상을 위한 여러 공학적 활동 중의 하나로, 안전사고가 발생한 후 사고의 원인을 파악하고 발생 과정을 이해함으로써 추후 동일한 혹은 비슷한 사고가 발생하지 않도록 시스템/직무/환경적 개선 요건을 도출하는 과정으로 정의된다.

3.2 위험성 평가: 사고가 발생하기 전 시스템 내에 존재하는 위험 요인을 도출해, 사고 위험도를 정량적 및 정성적으로 예측하고 이에 대한 효과적인 대비책을 마련하는 과정으로 정의된다.

3.3 안전-I과 안전-II: 안전-I은 전통적인 안전에 대한 개념으로 부정적인 일(사건 및 사고)의 발생이 최소화된 상태의 안전으로 정의되고, 안전-II는 안전에 대한 새로운 개념으로 긍정적인 일 혹은 성공적인 일의 발생이 최대화된 상태의 안전으로 정의된다.

3.4 안전 복원 탄력성(Resilience): 시스템의 변화 속에서도 기능을 제대로 발휘하는 시스템의 본질적인 능력으로 정의된다. 안전 복원 탄력성은 예상하지 못한 상황에서 시스템의 기능이 원활하게 수행될 수 있음을 보장한다.

3.5 기능 공명(Functional Resonance)과 FRAM: 시스템의 각 기능(직무)은 변동성(variability)을 가지고 있으며, 기능들의 변동성은 결합을 통해 시스템 변동성을 증폭시키거나 축소 시킨다. 기능의 변동성이 결합을 통해 시스템 전체 변동성에 영향을 주는 현상을 감지할 수 있는 신호를 기능 공명이라 정의한다. 기능 변동성 파급 분석법(FRAM: Functional Resonance Analysis Method)은 기능 공명을 분석하기 위해 개발된 시스템의 모델링 기법이다.

3.6 WAI와 WAD: 상정된 작업(WAI: Work-As-Imagined)은 시스템 설계자가 특정 상황에서 시스템의 기능(직무)이 수행되어야 하는 작업방식으로 정의되며, 실제적 작업(WAD: Work-As-Done)은 특정 상황에서 시스템의 기능(직무)이 실제로 수행되는 작업방식으로 정의된다.

3.7 ETTO 원칙(Efficiency-Thoroughness Tradeoff Principle): 사람은 작업을 할 때 이용 가능한 자원(시간, 정보, 기기 등)을 고려해서 효율성과 완전성 사이에서 상충 점을 찾아 적절하게 현재 작업 상황에 적응해가면서 작업하는 현상을 에토 원칙이라 정의한다.

3.8 역병적 모형(Epidemiological model): “사고는 분명하거나 또는 잠재적인 요소(latent factors)들이 결합되어 발생한다.”라고 가정하여 분석하는 모형으로 정의된다.

3.9 그 밖에 이 지침에서 사용하는 용어의 정의는 이 지침에 특별한 규정이 있는 경우를 제외하고는 산업안전보건법, 같은 법 시행령, 같은 법 시행규칙, 산업안전보건기준에 관한 규칙에서 정하는 바에 의한다.

4. 사고 분석 기법

4.1 전통적 기법

4.1.1 근원 분석(RCA)

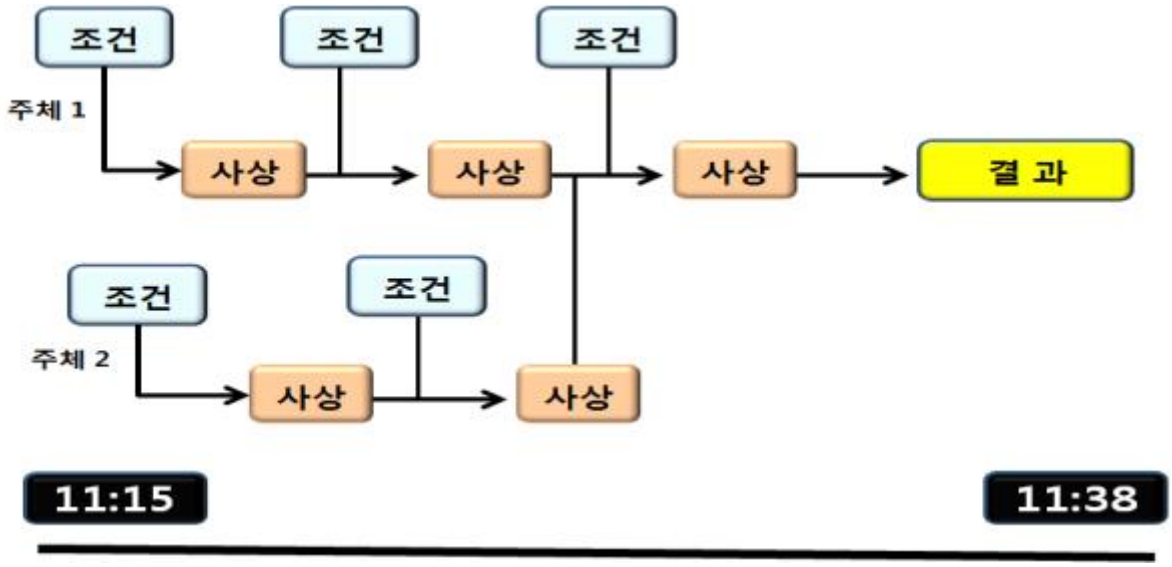
(1) 근원 분석 모형(기법)이란 문제의 진원을 찾고 그 원인을 제거하던가 아니면 예방하는데 초점을 맞추는 기법으로, 유의할 점은 징후(symptoms)를 다루는 기법이 아니라는 점이다.

(2) 브레인스토밍 방식에서부터, 파레토 차트, 통제 차트, 히스토그램, Mort(Management Oversight Risk Tree), 5-Why 그리고 6-sigma까지 다양하다. 한국산업안전공단 '사고의 근본원인 분석기법에 관한 기술지침'은 유익한 정보를 제공한다.

4.1.2 선형 원인-결과 기법

(1) 연속(순차)적 사상 기반(Sequential Event-Based) 기법은 순간순간 일시적으로 발생하는 사고 요인들을 인과관계로써 연결하여 사고/사건 발생의 원인을 설명하는 기법이다. '도미노 모형 (Domino Model)'이 대표적이다.

(2) 시간 순서 사상(Time-Ordered Events) 기법은 시간 순서에 따른 연속적 사상을 행동 주체(actor)별로 표시하는 기법이다. 시간별로 각 주체 중 어느 누가 사상에 관여하였으며, 이 사상들이 어떻게 영향을 받아 사고라는 결과가 발생했는지를 시각적으로 보여주는 장점이 있다. 대표적 모형은 MES(multi-linear events sequencing)이다.



<그림 1> 시간 순서 사상 기법

(3) 결함수 분석법(FTA; Fault Tree Analysis)은 해저드 분석(hazard analysis)에 적용되는 기법으로 사고를 발생시키는 원인들의 관계를 연역적-하향접근(Deductive & Top-down Approach) 논리를 사용하여 나뭇가지 모양 그림으로 나타낸 FT(Fault Tree)를 만들고 이에 의거하여 사상 발생 확률을 계산하여 안전 시스템의 신뢰도를 개선하는 정량적 평가 방법이다.

(가) 시각적으로 이해하기 쉽고, 또한 유연적이며, 분석대상의 위험성에 대한 확률론적인 정량평가도 가능하여 기존의 감각적, 경험적 사고로부터 탈피하여 논리적이고 확률론적인 정량적 결과를 도출할 수 있는 장점도 있다.

(나) FT 실행 절차는 분석 대상 시스템의 특성이나 목적, 분석 수준 목표에 따라 다소 차이가 있으나 일반적으로 6-단계로 이루어집니다. (산업안전공단 FTA 지침 참조)

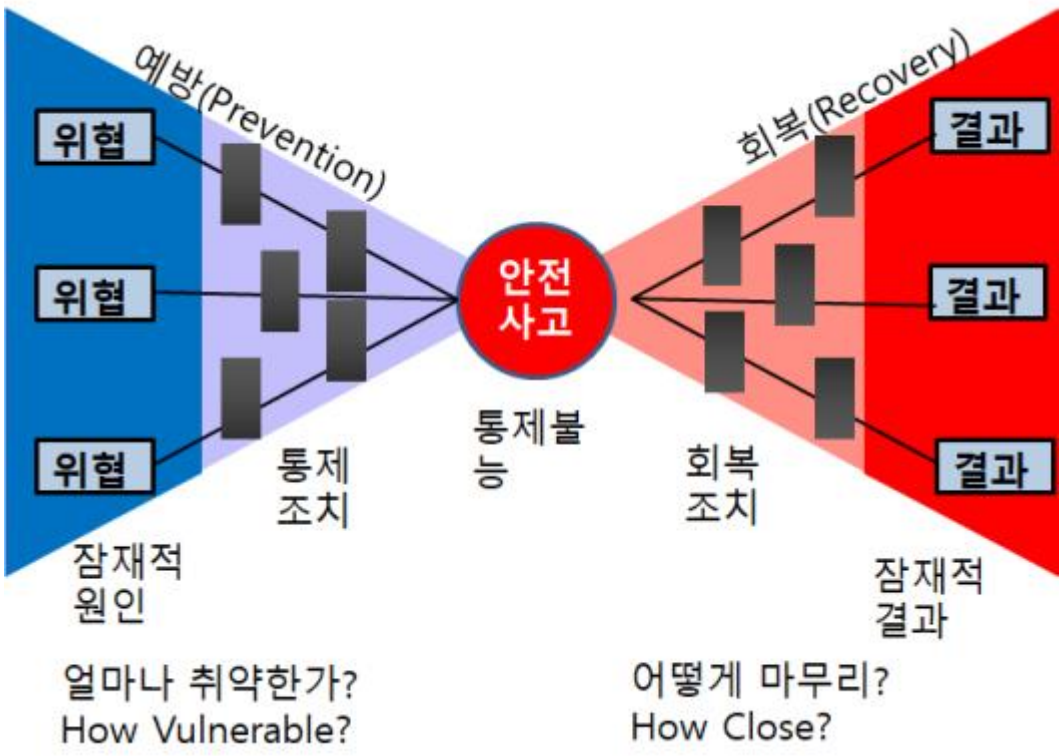
(4) 고장 형태 영향 분석(Failure Mode and Effects Analysis) 역시 해저드 분석(hazard analysis)에 적용되는 기법으로 발생 가능한 고장(Failure)과 이러한 고장으로 인해 야기될 수 있는 위험을 구조화하여 사전에 사고를 방지하는 기법이다.

(가) FMEA는 FTA와는 달리 귀납적이고 상향식(Bottom-up approach) 특징을 가지고 있다.

(나) FMEA 기법은 ①초기개발 및 설계단계에서 시스템의 기능과 관련된 잠재고장 모드를 해석하는 시스템 FMEA, ②설계 단계에서 설계결함에 의해서 야기된 제품의 잠재고장 모드를 해석하는 설계 FMEA, ③제조 및 조립 공정상의 결함에 의해 야기된 제품의 잠재고장 모드를 해석하는 공정 FMEA로 구분된다.

(다) 그 후, 시스템 구성요소의 고장 발생도, 시스템에 대한 심각도(severty), 사고 검출도를 평가하여 각 구성요소 고장의 위험 순위(RPN: risk priority number)를 결정하고, 이후 대책을 마련하고 조치를 취한 후 재평가한다.

(5) 보우 타이(Bow-tie)모형 기법은 발생 빈도가 잦고 결과의 심각성이 높은 사고에 활용되는 원인-결과 분석 기법이다. 모형 모양이 남자들이 이용하는 나비넥타이와 같아 이러한 이름이 붙여졌다.



<그림 2> 보우 타이 모형 기법

(가) 안전 분야에서의 보우 타이 모형은 안전사고(흔희 사상(Event)이라 부름)을 중심으로 왼쪽에는 사고의 원인과 관련된 시나리오를, 오른쪽에는 사고의 결과와 관련된 시나리오를 표기한다.

(나) 통제 조치(예방대책이라 칭하기도 함)은 원인과 사상 사이에, 그리고 회복 조치(감소대책이라 칭하기도 함)은 사상과 결과 사이에 각각 표기한다.

(다) 보우 타이 모형은 예방 차원에서의 통제 조치가 실패할 경우 어떠한 회복 조치가 필요하며, 각 조치에 따른 다양한 결과도 시각적으로 보여주는데, 이때 통제 조치가 실패되는데 작용하는 요소를 악화요소(Escalation factor)라 부르며, 이 악화요소를 방지할 수 있는 통제 조치들이 있는데, 이를 악화요소 방지통제(Escalation factor control)라 부른다.

4.1.3 역병적 기법

(1) 스위스 치즈 모형(Swiss Cheese Model)기법은 안전사고는 근로자 개개인을 대상으로 하여 분석하는 개인별 접근 방식(Person Approach)보다는 안전사고 관련 다양한 요인들을 역병적으로 분석하는 접근 방식이 효율적이라는 전제하에 제임스 리즌(James Reason)이 제시한 사고분석 기법이다.

(가) 안전사고는 단순히 한 요인에 의해서가 아니고 반듯이 여러 가지 결함에 의해 발생한다는 전제를 수용하는 것이 이 기법의 핵심이다.

(나) 다양한 요인들은 한장 한장의 치즈로 표현된다.

(2) 삼각대 베타(Tripod Beta) 모형 기법은 사고 발생을 방지하는 대책이 있음에도 불구하고, 안전 위험 요소가 대상(근로자 또는 설비)과 연계되어 사고가 발생되는 관계를 역병적으로 분석하는데 이용되는 기법이다.

(가) 위험 요소가 어떻게 스위스 치즈의 구멍(holes)을 통과하여 안전사고가 발생되는지를 설명하는데 유익하다.

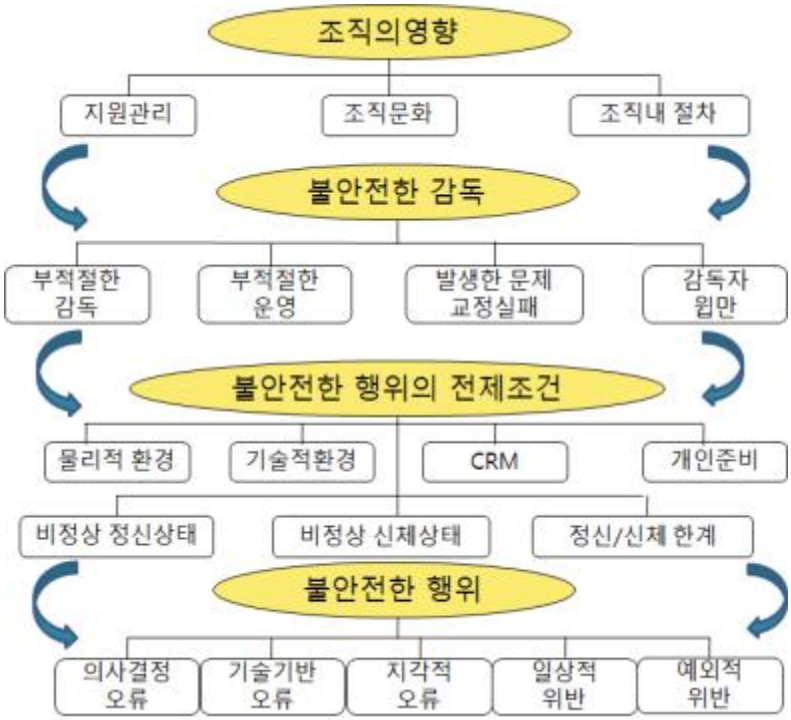
(나) '삼각대(Tripod)'라는 개념은 위험 요소, 대상, 그리고 이벤트(사고, 사상)로 구성된 'tripod trio's에서 유래한 용어이며, 특히 조직 구성원의 행동 모형과 연계되어 응용된다.

(3) HFACS(human factors analysis & classification system), HFACS 모델은 인적 오류로 인한 사고의 발생을 조직의 영향, 불안전한 감독, 불안전한 행위의 전제조

건, 불안전한 행위의 4단계로 구분한 스위스치즈모델을 기초로 하였다.

(가) 산업의 특성에 맞게 총 19가지 세부항목으로 분류하였다.

(나) 세부사항 구조는 다음과 같다.



<그림 3> HFACS 세부사항 구조

4.2 현대 기법

4.2.1 ETTO(Efficiency-Thoroughness Trade-Off) 원리

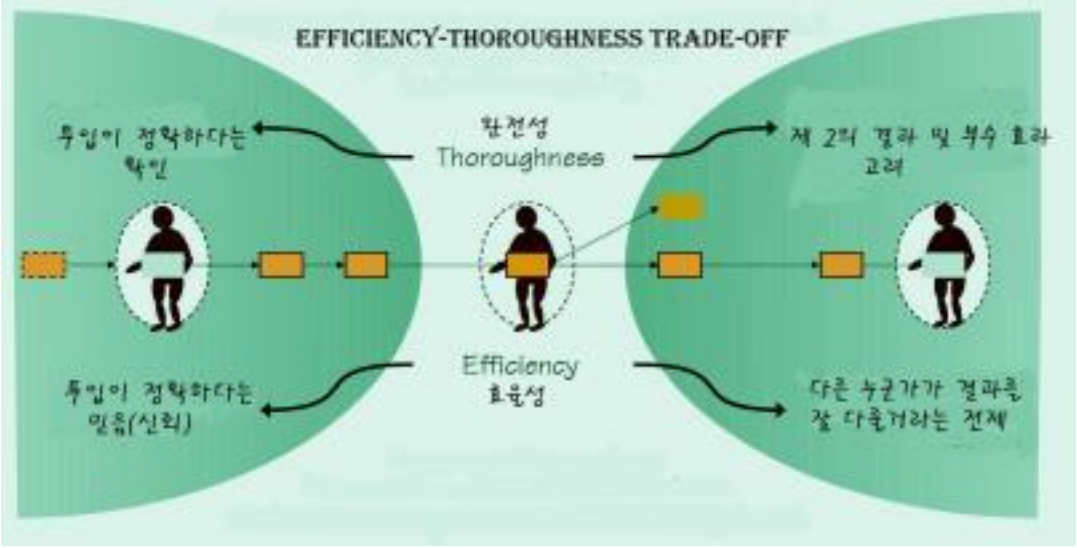
(1) 기술과 인간이 복잡하게 엮여있고, 그 관계성도 불확실한 여건에서는, 개인 및 조직은 효율성(efficiency)과 완전성(thoroughness) 사이에서 절충점을 찾는 적응적 전략을 선택한다.

(가) 효율성은 그 정의에서 알 수 있듯이 직무 목적을 달성하기 위해 사용되는 자원의 양을 최소화하는 것이며, 완전성은 직무 목적의 성공적 달성을 위한 모든 필요조건을 충족하는 것이다.

(나) Hollnagel은 이 두 개념은 동시에 극대화될 수는 없기에, 작업 운영자들은 절충점을 찾아 직무를 수행하는 전략적 행위를 보이는데, 완전성이 너무 강조되어 직무수행이 너무 늦어지는 경우와 효율성이 너무 강조되어 직무 수행이 부적절한 결과를 낳는 경우에 시스템에 실패(안전 사고)가 발생한다.

(2) ETTO 원리는 효율성과 완전성의 균형을 잘 유지하기위해 개인 및 조직이 전향적으로 사용하는 객관적이면서 정련된 전략의 집합체로 작업 수행의 변동성을 강조한다.

(3) ETTO 원리는 인적오류에 의한 안전사고를 분석할 경우 안전사고의 근원에 대한 새로운 시각을 제공하고 개인 및 조직의 직무 수행 전략을 성공적으로 만드는 요인을 이해하는 데 매우 유용한 서술적 모형이다.



<그림 4> ETTO 원리

4.2.2 STAMP/STPA

(1) STAMP (Systems-Theoretic Accident Model and Process) 기법은 안전사고는 일련의 사건이 연결고리와 같이 엮이는 것이 아니라 시스템 관점에서 통제 및 의사소통의 부적절 혹은 불충분한 결과로 발생한다고 강조한다.

(2) STAMP는 ①안전 제약 사항(Safety Constraints), ②적절한 계층적 구조화

(Hierarchical Safety Control Structure), ③프로세스 모델(Process Model)이라는 세 가지 개념에 기반을 둔 새로운 사고 평가 모델로 시스템의 개발과 운영에 관여하는 모든 요소들을 포함합니다.

(3) STAMP 모델의 안정성 분석을 위해 개발된 STPA(System-Theoretic Process and Analysis)은 시스템을 위험으로 이끄는 원인을 밝혀내는 목적으로 4단계의 절차를 통해 수행된다.

(가) 1단계는 시스템의 위험이 구체적으로 무엇인지를 명확히 정의하는 과정이다.

(나) 2단계는 시스템의 통제 구조(control structure)를 그리는 과정이다.

(다) 3단계는 시스템을 위험으로 이끄는 부적절한 제어를 밝혀내는 과정이다.

(라) 4단계는 STPA의 위험한 제어를 일으킬 수 있는 원인을 발견하는 과정이다. 위험한 제어와 관련하여 원인으로 4가지가 있다.

<그림 5> STPA 위험한 제어 관련 원인

4.2.3 FRAM(Functional Resonance Analysis Model)

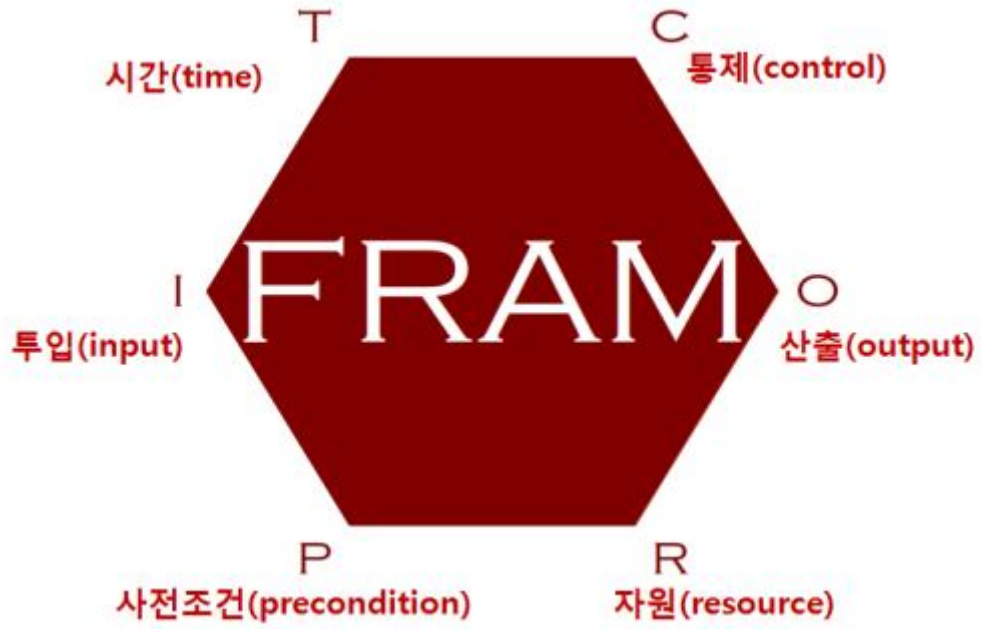
(1) 이 기법은 안전사고가 발생하는 과정을 시스템 기능들의 비선형적인 상호작용을 이해하고 예측하는 기법으로써 시스템 운영에서 변동성(variability)은 필연적이며, 동일 프로세스와 전략적 행위를 하여도 성공과 실패는 모두 발생할 수 있다

는 개념이 FRAM의 기본 철학이다.

(2) FRAM에서의 기능적 공진(functional resonance)은 바람직하지 못한 사상(event)을 암시하되 감지할 수 없는 여러 신호의 약한 변동성이 의도하지 않은 상호작용을 해서 어떻게 감지 가능한 사건의 신호로 창발적 과정을 통해 발전해 가는가를 설명하는 개념이다.

(3) FRAM은 변동성을 서술하고 의도하지 않은 변동성을 억제하기 위해 일반적으로 4단계를 거친다.

(가) 1단계: 시스템의 필수적인 기능을 파악하고 이 기능들을 6개요인(시간, 통제, 투입, 산출, 자원, 사전 조건)으로 특성화한다.



<그림 6> FRAM 기능

(나) 2단계: 공통 수행 조건(common performance conditions (CPC))과 변동성의 현상적 형태(variability phenotypes)를 활용해서 상황 의존적인 수행 변동성을 특성화 한다. 일반적으로 11개의 CPC를 활용한다:

① 인력 및 장비 이용 가능성
② 훈련, 핵심역량, 사전 준비성
③ 의사소통 수준
④ 설비 및 운영 지원

⑤ 사전 조건의 이용가능성
⑥ 작업 조건
⑦ 목표와 갈등
⑧ 이용 가능 시간
⑨ 스트레스
⑩ 팀 협동
⑪ 조직 수준

(다) 3단계: 기능들의 가능한 의존성 및 유기론적 관계에 근거해서 기능적 공진을 정의한다. FRAM에서의 각 기능은 6개의 측면에서 특성화되기에 기능들이 다양한 방법으로 연결되고 상호작용이 이루어진다.

(라) 4단계: 안전이 위협받을 수 있는 변동성에 대해 장벽(barriers)을 파악하고 수행도를 모니터링할 수 있는 척도나 요건을 개발한다. 4 가지의 장벽 시스템을 활용한다.
① 물리적 장벽(physical barrier system)
② 기능적 장벽(functional barrier system)
③ 상징적 장벽(symbolic barrier system)
④ 무형의 장벽(incorporeal barrier system)

4.2.4 인지 공학(Cognitive Engineering) 모형

(1) 인지 공학 모형이란 시스템 내에서 인간의 (인지적) 행위와 기계 시스템 사이의 상호작용을 체계적으로 다루는 모형으로 직무 수행 과정에서 발생 가능한 오류 유형 파악이나 오류 유발 원인 구조 등 정성적 오류 분석과 인적오류 발생 상황 정보에 근거한 정량적 평가를 중시한다.

(2) 대표적인 모형으로 HRMS(Human Reliability Management System), CREAM(Cognitive Reliability & Error Analysis Method), EID(Ecological Information Design) 모형 등이 있다.

5. 사고분석의 기본적 개념

5.1 전통적 사고분석 개념

5.1.1 기존의 안전 사고분석에서의 안전 개념은 소위 안전-I으로 다음의 특징을 갖는다.

(1) 시스템의 부정적 결과(예: 사고)가 존재하지 않는 상황을 안전으로 정의한다.

(2) 'find and fix(찾아서 고치기)'로 알려져 있다. 즉, 실패 혹은 고장이 발생하면 그것의 원인을 찾으려고 노력하고 원인을 찾은 후에 그 원인을 제거하고 방벽(barriers)을 개선한다.

(3) 시스템의 구성요소와 그것들이 어떻게 작동 혹은 실패하는가를 조사함으로써 시스템을 이해할 수 있음을 가정하고, 또한 성공하게 되는 경우의 원인이 실패하게 되는 경우의 원인과 다름을 가정한다.

5.1.2 안전-I에 기반한 사고분석은 다음의 한계점이 있다.

(1) 이분법적인 세계관 및 결정론적인 세계관: 실패의 원인과 성공의 원인이 다르다는 관점과 사고는 특정 경로를 거쳐 발생하게 되어 있다는 관점

(2) 근본 원인에 대한 맹신과 간단하면서도 그럴 듯한 스토리의 맹신: 선형적 인과관계 모형에의 강한 의존

(3) 사고 원인 탐색 과정에서의 확인 편향(confirmation bias)

(4) 사고분석에서의 사후 확신 편향(hindsight bias)

(5) 사고에 관계된 부정적 결과에만 집중함으로써, 사고에 관계 없지만 문제가 있었던 요소를 간과하게 되는 경향

(6) 비난할 대상을 찾기에 집중

(7) 인적오류는 잘못된 시스템 설계의 증상이 아닌 사고의 직접적 원인이라 믿는 시각

5.2 현대 사고분석 개념

5.2.1 긍정적 결과(예: 사고 예방)가 존재하는 상황 소위 안전-II를 안전으로 정의한다.

5.2.2 안전-II의 특징은 다음과 같다.

(1) 안전을 안 좋은 결과의 최소화(혹은 부재)로 정의하지 않고 항상 성공적으로 시스템이 작동하는 상태로 정의한다(성공 경우의 수를 최대화).

(2) 시스템이 어떻게 정상적으로(성공적으로) 작동되는가를 이해할 필요가 있음을 강조한다. 그러나 실패 상황을 이해하는데도 노력을 기울일 필요가 있음도 강조한다.

(3) 시스템이 성공하는 이유는 사람과 조직이 주어진 상황에 잘 대응하기 위해 그들의 작업을 지속으로 조정하기 때문임을 강조한다.

6. 현대적 사고분석을 위한 지침(P-D-C-A)

6.1 사고분석 계획(PLAN)

6.1.1 오늘날 사고분석에서 시스템적 접근법 혹은 시스템적 사고가 많이 강조되고 있는데 이는 안전-II 기반의 사고 분석이다.

6.1.2 필수적으로 요구되는 10개의 시스템적 사고의 원칙은 다음과 같다.

(1) 원칙-1: 현장 전문가의 참여(Involvement of field experts)

(가) 실제 작업(WAD)을 이해하기 위해 실제로 작업을 수행하는 현장의 전문가를 분석 조사 과정에 참여시켜야 한다.

(나) 전문가의 다양한 의견을 종합해서 WAD를 이해해야 한다.

(2) 원칙-2: 국소적 합리성(Local rationality)

(가) 작업자가 작업을 수행할 때 주어진 상황에 맞추어 자신의 목표, 지식, 시스템 상황의 이해 등을 바탕으로 합리적이라고 생각되는 행동을 한다.

(나) 사고분석 과정에서 이를 이해할 필요가 있다.

(3) 원칙-3: 공정문화(Just culture)

(가) 작업자는 좋은 결과를 내기 위해 자신의 최선을 다하지만 성공할 때도 있고 실패할 때도 있다.

(나) 작업자가 자신의 작업 수행에 대해 가감없이 다른 사람들과 공유할 수 있는 공정문화가 정립될 필요가 있다.

(4) 원칙-4: 작업요구사항(Demand and Pressure)

(가) 작업의 효율성과 능력에 관련된 작업 요구사항과 (시간) 압박은 작업 수행도에 결정적인 영향을 미친다.

(나) 작업 수행도는 작업 수행 당시의 요구되는 사항과 그로 인한 여러 압박감을 고려해서 조사될 필요가 있다.

(5) 원칙-5: 자원과 제약조건(Resources and constraints)

(가) 작업수행의 성공은 적절한 자원 및 적절한 제약조건에 의존한다.

(나) 작업의 요구사항에 대처하기 위해 인력, 정보, 장비, 절차서 등을 포함한 자원이 이용가능해야 한다.

(다) 이러한 자원과 관련된 제약조건이 적절하게 제공되었는가를 고려해야 한다.

(6) 원칙-6: 상호작용 및 흐름(Interactions and flows)

(가) 작업수행에 필요한 기능(직무)들간의 관련성 및 흐름을 이해해야 작업수행 방법 및 결과를 올바르게 이해할 수 있다.

(나) 시스템을 구조적 관점과 더불어 기능적 관점에서도 이해할 필요가 있다.

(7) 원칙-7: 상충효과(Trade-offs)

(가) 시스템의 복잡성과 불확실성, 외부의 환경변화 등에 대처하기 위해 작업자는 상충하는 작업목표들의 절충점을 찾아 행동한다.

(나) 작업자 행동을 이해하기 위해 ETTO 원칙을 이해한다.

(8) 원칙-8: 수행 변동성(Performance variability)

(가) 주어진 작업 상황에 대처하기 위해 작업자는 지속적으로 적응 및 조정해가면서 작업하면서(performance adjustments) 수행변동성이 생긴다.

(나) 수행변동성으로 동일한 작업이 실패하기도 하고 성공하기도 한다.

(다) 이런 점이 사고 분석 과정에서 고려되어야 한다.

(9) 원칙-9: 발현적 현상(Emergence)

(가) 시스템에서의 수행도는 단순한 선형적 인과관계에 의해 결정되고 설명되는 것이 아닌 일종의 발현현상으로 간주되어야 한다.

(나) 이러한 이유로 수행도가 예상한대로 이루어지지 않고 이해하기 어려운 경우가 발생한다.

(10) 원칙-10: 동일성(Equivalence)

(가) 작업의 성공과 실패는 같은 원인으로부터 시작된다.

(나) 이러한 이유로 오로지 실패한 경우만 분석하는 것은 맞지 않고 어떻게 작업 수행도가 변동해가는가를 분석하는 것이 더 옳은 접근법이다.

6.2 사고분석 실행(DO)

6.2.1 안전-II의 개념을 사고분석에 도입하고자 함은 안전-I의 한계점을 보완하자는 것이지 안전-I을 대체하자는 것이 아님을 이해할 필요가 있다.

6.2.2 사고분석에서 안전-I과 안전-II가 각각 갖고 있는 장점이 있으므로 이를 통합적으로 활용할 필요가 있다.

(1) 사고분석 기법에서 사고모형 혹은 인과관계 모형을 가정하고 있으면 사고분석 과정의 효율성을 높여줄 수 있다. 그러나 이러한 모형의 가정은 실제적 상황과 다를 수 있음을 항상 인지하고 사후확증편향과 같은 인지적 편향에 빠지지 않도록 해줄 필요가 있다. 사고모형에 근거한 분석 결과는 참고할 수 있는 정보 정도로 인식하는 것이 필요하다.

(2) 사고분석 기법에서 가정하는 인과관계 모형은 그 방법의 사용을 제약한다. 따라서 분석자는 그 모형의 가정 및 인과관계의 관점에서 모든 사고를 바라볼 가능성이 높다. 이를 극복하기 위해 사고분석 방법은 인과관계 모형의 사용에 너무 의존해서는 안되며 정상적인 시스템 기능 모형을 사용할 필요가 있다. 이는 성공적인 결과와 실패적인 결과가 결국은 같은 행위적 동기에서 비롯된다는 안전-II의 사상을 적극 반영한 것이다.

(3) 사고분석 기법에서 사고의 원인으로 고려될 수 있는 실패 유형의 분류체계를 제공한다면 분석자는 그 분류체계의 내용을 활용해 사고의 잠재적 원인을 결정할 수 있고 분석과정의 효율성은 높아질 수 있다. 그러나 위의 첫 번째 항목과 마찬가지로 제공되는 분류체계의 내용 이외에 다른 원인이 충분히 있을 수 있음은 항상 인지할 필요가 있다.

(4) 작업자 관련 사고의 원인으로 인적오류 외에 다른 유형의 요소가 충분히 가능성이 있을 수 있으므로 모든 사고분석의 궁극적인 결과가 인적오류의 규명이 되도

록 해서는 안된다.

(5) 사고분석 기법은 분석자가 오로지 하나의 근본원인을 찾는 것에 몰두하지 않도록 해야 하며 가급적 가능한 많은 원인을 파악할 수 있도록 도와줘야 한다.

(6) 사고분석 기법에서 제공하는 실패(혹은 원인요소)의 분류체계는 인간의 활동에 관련된 개념적으로 탄탄한 이론 및 프레임워크에 기반해서 정의된 것을 활용할 필요가 있다.

(7) 분석대상의 사고를 광범위하고 철저하게 표현하고 분석하기 위해 분석의 단위는 개인, 팀, 조직, 사회적 요소, 문화적 요소, 기술적 요소 등을 모두 포함하는 전체 사회-기술 시스템이 될 필요가 있다.

(8) 분석대상이 되는 사고가 낮은 수준의 사고이건 높은 수준의 사고이건 그 추상적 수준 혹은 규모에 관계없이 사고 분석 기법은 일관성 있게 활용될 수 있어야 한다.

(9) 사고분석 기법은 작업자는 항상 자신이 이용할 수 있는 (인지적) 자원을 활용해 당면한 작업요구사항을 해결하기 위해 동적으로 자신의 수행과정을 조절 및 적응해간다는 사실을 반영할 필요가 있다. 이를 위해 분석 기법은 분석자로 하여금 사고분석 과정에서 사고에 직간접적으로 연관되어 있을 다양한 상황적 인자를 고려할 수 있도록 도와줘야 한다.

(10) 사고분석 기법은 발생한 사고와 관련된 시스템의 기능들간의 선형적 인과관계 혹은 특정 원인요소들의 선형적 인과관계로 충분히 설명될 수 없다는 가능성을 받아들일 수 있어야 한다. 사고가 인과관계의 결과가 아닌 발현적 현상의 결과임을 인정할 수 있어야 한다. 이를 위해 안전-II의 개념 중 변동성 및 이의 파급현상을 중점적으로 활용할 필요가 있다.

(11) 동일한 현상의 사고라도 다른 원인과 과정에 의해 발생할 수 있다. 따라서 사고분석 기법은 동일한 현상의 사고가 항상 동일한 원인과 과정에 의해 발생한다고 분석자가 기계적(맹목적)으로 분석하지 않도록 해야 한다.

6.3 사고분석 검토(CHECK)

6.3.1 다음의 항목을 중심으로 안전-I 기반의 사고분석의 약점을 어느 정도 보완하고 있는가를 점검한다.

(1) 작업 성공의 원인과 실패의 원인이 다르다는 이분법적 관점을 여전히 유지하지는 않았는가를 점검한다.

(2) FRAM과 같은 안전-II 기반의 사고분석 기법을 활용하면서 근본원인 찾기에 집중하고 있지 않았는지를 점검한다.

(3) 사고 원인 탐색 과정에서의 확인 편향(confirmation bias)에 빠지지 않았는가를 점검한다.

(4) 사고 분석에서의 사후확신편향(hindsight bias)에 빠지지 않았는가를 점검한다.

(5) 사고에 관계된 부정적 결과에만 집중함으로써 사고에 관계 없지만 문제가 있었던 요소를 간과하지는 않았는가를 점검한다.

(6) 근본원인과 연계해서 비난할 대상을 찾기에 집중하지 않았는가를 점검한다.

(7) 인적오류를 사고의 원인으로 지목하는 경향을 보이지는 않았는가를 점검한다.

6.3.2 사고는 선형적 인과관계 모형에 기반하는 현상이 아닌 여러 요인들의 복합적 상호작용으로 발현적으로 출현한 현상임을 지속적으로 견지했는가를 검토한다.

6.3.3 사고분석에서 기능(직무) 수행과정에서의 변동성 및 기능간 변동성 파급효과를 고려해서 사고발생 과정을 이해했는가를 검토한다.

6.3.4 사고분석의 결과를 활용해서 직무절차, 작업환경, 작업시스템 등을 개선할 때 기능(직무)수행의 변동성을 감소시킬 수 있는 방향으로 개선안을 도출했는가를 검토한다.

6.4 사고분석 개선(ACT)

6.4.1 안전-II 기반의 사고분석을 통해 안전-I 기반의 사고분석의 약점을 얼마나 잘 보

완했는가를 검토해 이를 향후 사고분석에 반영한다.

6.4.2 주기적으로 사고분석을 얼마나 잘 진행하고 있는가를 검토해서 이를 사고분석 과정에 적극 반영한다.

KOSHA GUIDE
Z - 29 - 2022

지침 개정 이력

□ 개정일 : 2022. 12. 29.

○ 개정자 : 한국안전문화진흥원

○ 개정사유 : 가이드라인 고도화

○ 주요 개정내용

- 1. 목적 변경
- 2. 적용범위 변경
- 3. 용어의 정의 변경
- '4. 기본사항' 삭제 후 '4. 사고 분석 기법' 추가
- '4.1 전통적 기법'과 '4.2 현대 기법' 추가
- '5. 사고분석의 기본적 개념 및 세대별 사고분석 기법의 특징'을 '5. 사고분석의 기본적 개념'으로 변경
- '6. 사고분석을 위한 지침'을 '6. 현대적 사고분석을 위한 지침(P-D-C-A)'으로 변경
- '6.2 안전-I 및 안전-II의 통합적 균형에 기반한 사고분석(DO)'을 '6.2 사고분석 실행(DO)'으로 변경
- '6.2.3 안전-II의 핵심적 개념 중의 하나인 기능 수행에서의 변동성을 중심으로 사고분석이 필요하다면 기능 변동성 파급효과 분석법(FRAM)을 활용해볼 수 있다.' 와 '6.2.4 안전-II 기반의 사고분석을 위해 FRAM을 활용한다면 다음의 사항을 염두에 둘 필요가 있다.' 삭제