산업 안전시스템에 있어서 Fault Tree Analysis의 적용
—An Application of Fault Tree Analysis in Industrial Safety System—

김 진 규*

ABSTRACT

Fault tree analysis(FTA) is available to the engineer for determining reliability of complex industrial safety system. Therefore quantitative aspects of FTA greatly multiply its power. this paper proceeds of presenting the methodology of FTA, including an approach to constructing in fault tree. A working guide to the use of FTA for the purpose of cost/benefit determination in industrial safety system is given. Finally, an analytic method for uncertainty analysis of the top event of a complex system is described.

1. 서 론

정치적·사회적·환경적 관점에서의 안전에 관한 의문점은 오늘날 산업기술이 급속하게 발달된 우리 사회가 요구하는 과학의 목적과 일치하게 된다. 이와 같은 목적을 달성하기 위해서 시스템의 신뢰성과 안전성 분석을 실시할 필요가 있게 되었다. 또한 산업안전 시스템에서는 하나의 인간 error와 기계장치의 고장이 곧 큰 사고가 되는 경우도 있으나, 여러가지 사상이 중복된 결과로써 큰 사고로 되는 것이 전형적이다. 이와 같이 어느 정도 복잡한 인간—기계계(man-machine system)의 안전대책과 사건의 조사·예측은 임기 응변적인 대책만으로는 감당할 수가 없게 되었다[2,3]. 이와 같은 복잡한 산업안전 시스템의 신뢰성과 안전성을 결정하고, 이를 수학적으로 해석해 나가는 유용한 기법이 바로 FTA(Fault Tree Analysis) 기법이다.

FTA의 목표는 원래 재해와 사고의 발단을 확률적인 수치로 하여 평가하는데 있다. 따라서 이 FTA를 재해요인 분석과 대책에 응용하기 위해 수학적으로 해석하는 부분을 제외하면 해석하여야 할 재해사례와 재해요인 및 재해요인의 상호관계를 정확하게 연역적으로 도식화하여 추구할수가 있다. 이를 토대로 안전대책을 이론적으로 검토할 수가 있으므로써 재해방지에 극히 유효한 기법이라고 할 수 있다[1].

따라서 본 논문의 목적은 FTA 분석을 계량화해서 안전을 위한 예산을 효과적으로 할당하는 것이다. 이를 위해 다양한 대체적인 안전투자안을 FTA를 통하여 분석하여서 산업안전 관리자가 의사결정을 하는데 필요한 비용/효과의 척도를 제공하는 것이다. 궁극적으로 FTA의 기본개념과 사용하는 절차를 서술하며, 산업안전 시스템에서의 효과적인 예산을 할당하기 위한 비용/효과 결정을 통한 척도를 제공하는데 있다. 또한 FTA에 사용된 기본사상의 확률결정에 있어서 불확실성이 개입됨으로써 정상사상의 확률에 미치는 영향을 분석하는 해석적 모델을 제시한다. 불확실성 분석은 복잡한 시스템에서는 중요한 역할을 하는데, 이는 처음 개발된 시스템이거나 물리적 혹은 다른 변동요인에 의해 기본사상에 정확한 수치를 할당할 수가 없기 때문에 이루어져야 할 것이다[5].

2. FTA을 이용한 산업안전 시스템의 설계

2.1 FTA의 정의와 기본개념

FTA는 시스템의 고장을 체계적인 도식으로 탐색하여 어떤 부품이 시스템고장의 주원인 인가를 찾아내는 연

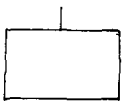
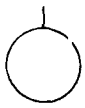
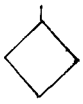
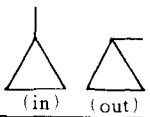
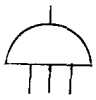
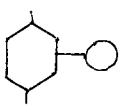
*한양대학교 산업공학과 박사과정

접수 1990년 4월 20일

역적인 해석기법으로 시스템의 고장요인들의 상호관계를 Boolean Logic Gate를 이용하여 도해식으로 표현하는 분석기법이다.

이 FTA는 1962년에 Bell 전화연구소의 H. A. Watson이 MLCS(Minuteman Launch Control System)의 안전성을 평가분석 할때 처음 사용하면서 부터 항공학, 원자력공학, 인간공학, 안전관리학 등 여러 다른 분야에 널리 보급되어서 연구되어 지고 있는 추세이다[4,11,12]. Fault Tree(FT)에 사용되는 기호에는 두 종류가 있으며 그 구체적인 내용은 다음의 〈표1〉과 같다[6].

〈표 1〉 FT 작성에 사용되는 기호

구분	기 호	명 칭	내 용 설 명
사상기호		결함사상	기본 고장의 결함으로 이루어진 고장의 상태
		기본사상	주어진 시스템의 기본사상
		기본사상Ⅱ	기본사상으로서 평가되었으나 그 결과가 상위의 사상에 삽입된 사상
		이하 생략의 결함사상	더 분석이 가능하나 기본사상으로 가정된 사상
		통상사상(집모양사상)	통상의 작업이나 기계의 상태에 재해발생 원인이 되는 요소를 나타내는 사상
		전이기호	다른 Gate로 들어오고 나가는 사상
논리기호		AND Gate	출력사상이 일어나기 위해서는 모든 입력이 일어나지 않으면 안된다는 논리조작기호
		OR Gate	입력사상의 어느 하나가 일어나도 출력사상이 일어난다고 하는 논리조작기호
		INHIBIT Gate	가정된 조건이 만족되면 입력사상이 곧바로 출력사상을 발생시키는 논리조작기호

2.2 FT의 작성 절차

FT는 다음과 같은 순서의 top-down approach로 작성해 나간다[9].

(1) 대상이 되는 시스템의 범위를 결정한다.

(2) 대상시스템에 관계되는 자료를 정비해 둔다.

(3) 상상하고 결정하는 사고의 명제(나무의 정상사상(head event))를 결정한다.

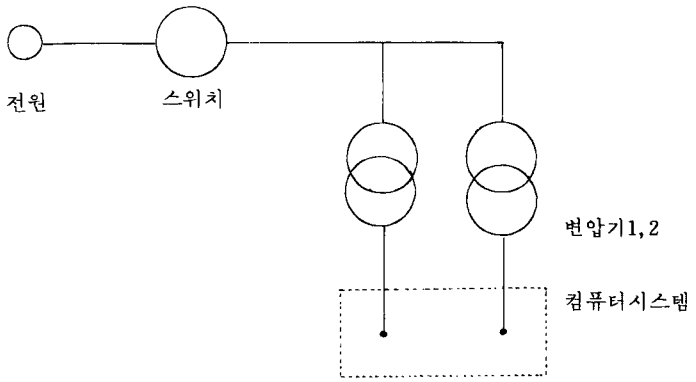
(4) 원인 추구의 전제조건을 미리 생각 해둔다.

(5) 정상사상에서 시작하여 순차적으로 생각되는 원인의 사상(중간사상 및 말단사상)을 논리기호로 이어간다.

(6) 먼저 골격이 될 수 있는 대충의 나무를 만든다.
나무에 나타나는 사상의 중요성에 따라 보다 상세한 부분의 나무로 전개한다.

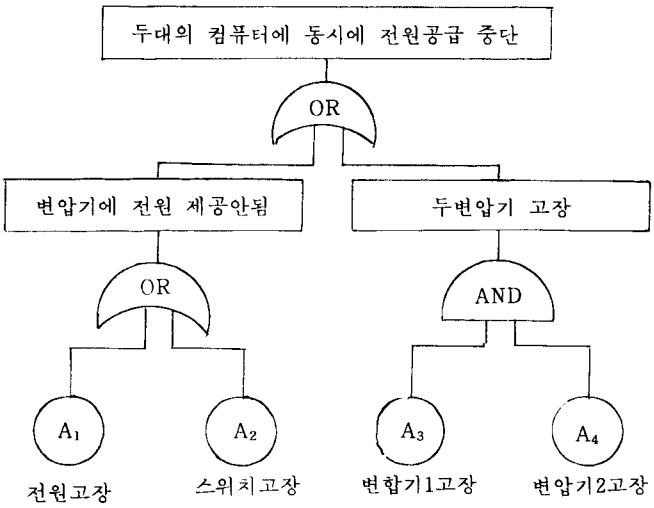
(7) 각각의 사상에 번호를 붙인다.

그러면 다음 〈그림 1〉과 같은 시스템을 고려하여 FT를 작성해 보자. 이 시스템은 중복설계된 두대의 컴퓨터에 전원을 제공하는데, 여기서 고장 사상은 동시에 두대의 컴퓨터에 고장이 일어나는 것이다.



〈그림 1〉 컴퓨터 시스템의 예

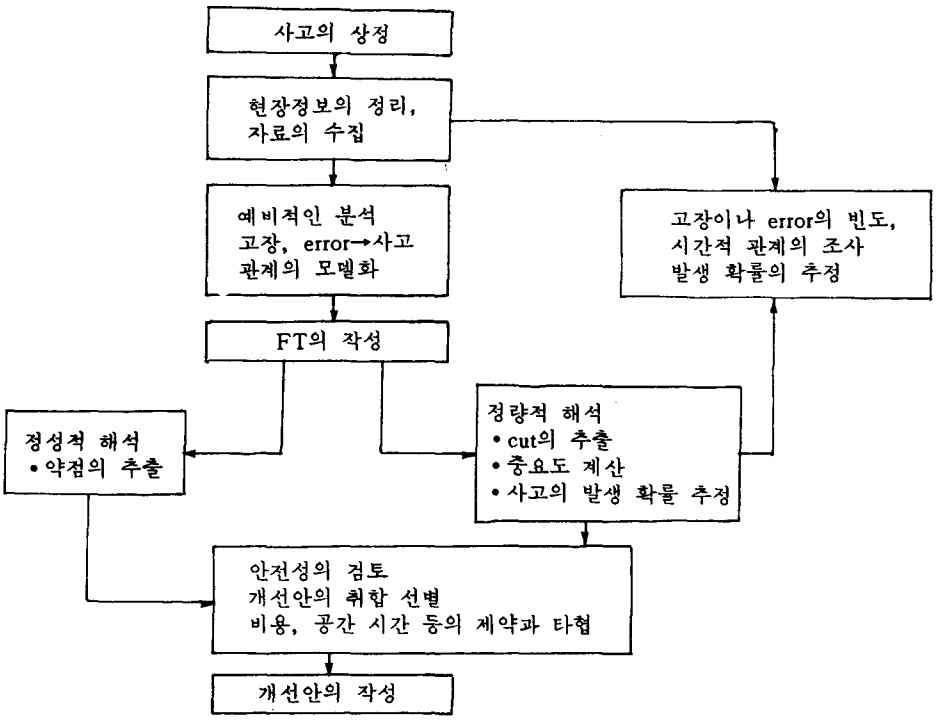
이 시스템에서 기본사상은 전원고장, 스위치고장, 변압기1,2 고장이다.
이것을 토대로 앞 절에서 서술된 FT의 작성절차에 따라서 FT를 작성하면 다음 〈그림 2〉와 같다.



〈그림 2〉 컴퓨터 시스템의 FT작성 예

2.3 FTA의 분석절차

FTA의 분석절차는 일반적으로 1) 시스템의 정의 2) FT의 작성 3) FT 평가순으로 이루어진다. 이 분석절차를 D. R Cheriton이 제시한 순서로 하여 그림으로 나타내면 아래 〈그림 3〉과 같다[1,8,12].



〈그림 3〉 FTA의 분석 절차

2.4 FT의 용도

FT는 다음과 같은 여러 가지의 정성적, 정량적 분석을 하는데 쓰여 진다[1,6].

(1) Mininmal cut set을 이용하여 시스템의 신뢰성, 체계적인 순서, 확률 순서를 구하여 시스템의 안전도를 파악할 수 있다. 여기서 cut set이란 정상사상을 유발시키는 기본사상의 교접(intersection)으로 표시되어 진다. Cut set 중 중복되어 지는 부분을 제거한 후 남은 set를 minimal cut set의 연합으로 표시한다. 이 연합에서 상향식(bottom up approach) 또는 하향식(top down approch)으로서 minimum cut set을 구할 수 있다.

(2) 고장을 연역적으로 찾을 수 있다. 그러므로 직관적 방법이나 귀납적 방법으로 찾을 수 없는 예상되는 cut set을 찾을 수 있다.

(3) 시스템의 고장난 부분을 쉽게 찾을 수 있다.

(4) 그 밖에도 시스템을 체계적으로 도해시켜서 면밀한 고장 연구나, 설계변경 등을 용이하게 할 수 있다.

3. 비용/효과 결정을 통한 산업재해 시스템의 안전성 분석

비용/효과의 용어는 음효율(negative utility) 감소당 소비된 비용으로 정의된다. 효과의 척도는 기대 음효율 감소(expected negative utility reduction)로서, 음효율은 모든 사고의 심각도(severity)에 직접적으로 의존한다. 음효율은 과거의 자료로 부터 얻어진 정상사상의 빈도수로서 나타내진다. 예를 하나 들어보면 〈표 2〉와 같다[6].

〈표 2〉 음효율의 예

삼각도 분류	심 각 도	음효율 Ui
1	응급처치(First Aid)	20
2	순간적인 전체고장(Temporary Total)	345
3	영구적인 부분고장(Permanent Partial)	2,500
4	영구적인 전체고장(Permanent Total)	21,000

정상사상의 기대음효율 E는 〈식 1〉과 같다.

$$E=\sum_{i=1}^{N} P_i * U_i \quad \cdots\cdots \langle 1 \rangle$$

단, pi : 정상사상이 일어날때 i번째 분류의 심각도가 일어날 확률

N : 심각도 분류의 수

E값은 또한 어떤 사고의 기대비용이라고 할 수도 있다. 여기서 만약 정상사상의 과거 출현횟수 n을 알 수 있다면 기대음효율 E는 다음과 같이도 나타낼 수도 있다.

$$E=\frac{\sum_{i=1}^{n} U_i}{n} \quad \cdots\cdots \langle 2 \rangle$$

정상사상의 확률 P값이 주어졌다면, 주어진 생산기간 동안에 정상사상에 관련된 기대음효율 즉 절대적인 위급도(*absolute criticality*) C는 〈식 3〉과 같다.

$$C=P*E \quad \cdots\cdots \langle 3 \rangle$$

이것을 예로 들어보면,

어떤 정상사상이 과거 100mmh(million man-hours) 동안에 5번 일어났고, 이 사상의 평균 심각도는 〈식 1〉, 〈식 2〉에 의하여 8 lost work day라고 하면, C는 0.05 occurrence/mmh*8lost work days/occurrence로서 0.4 work days/mmh이다.

다음에는 정상사상의 확률 P값을 결정해 보자.

FT의 맨 마지막 가지 즉 기본사상의 확률을 사용한 P값의 결정은 다음 식들과 같다.

$$P_{OR}=1-\pi(1-P_i) \quad \cdots\cdots \langle 4 \rangle$$

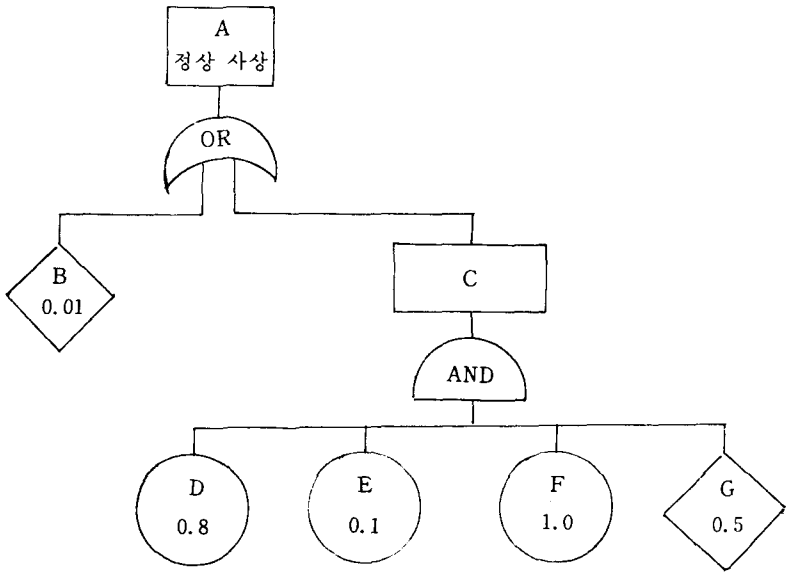
$$P_{AND}=\pi_{P_i} \quad \cdots\cdots \langle 5 \rangle$$

$$P_{NOT}=1-P \quad \cdots\cdots \langle 6 \rangle$$

$$P_{EXOR}=p_1+p_2-2p_1*p_2 \quad \cdots\cdots \langle 7 \rangle$$

여기서 P의 첨자는 Gate명이며, 이중 EXOR는 'y개중에서 x개 배제' 즉, 'exclusive x out of y'의 의미이다.

그러면 다음 〈그림 4〉와 같은 정상사상 확률 P를 구해 보자.



〈그림 4〉 FTA를 이용한 정상사상의 확률 계산 예

과거자료로 부터 이런 유형의 사건이 10번 일어나면 6번은 응급처치, 3번은 순가적인 전체고장, 그리고 나머지 1번은 영구적인 부분고장이다.

〈표 2〉의 음효율을 이용하여 기대음효율 E를 구하면 다음과 같다.

$$E=(0.6\times20)+(0.3\times345)+(0.1\times2500)=365.5$$

그리고 P는 〈식 4〉, 〈식 5〉를 이용하여 구하면,

$$P_{AND}=(0.8)\times(0.1)\times(1.0)\times(0.5)=0.04$$
$$P_{OR}=1-(1-0.1)\times(1-0.04)=0.0496$$

으로서 P는 0.0496이다.

따라서 정상사상 A의 위급도 C는 〈식 3〉에 나타난 바와같이

$$C=P*E=(0.049)\times(365.5)=18.1288$$

이다.

정상사상 확률 P를 줄이기 위해서 제안된 대체안에 대해서 앞에서 논의된 절차에 따라서 새로운 위급도를 계산하여 원래의 위기도에서 감하면 효과가 되고 이 값으로 비용을 나누면 이것이 비용/효과의 값이 된다. 모든 대체안들 가운데서 안전재해 예산이 허용되는 한도 내에서 최소의 비용/효과 값을 가진 대체안을 선택하면 최선의 안전재해 방지책이 될 것이다.

만약 예산이 시스템의 안전도를 향상시키기 위해서 투입된다면 FT에서 기본사상의 확률들은 감소될 것이며, 이로 말미암아 기대심각도(expected severity)가 감소할 것이다. 기본사상의 확률감소는 정상사상의 확률을 향상시켜 줄 것이며, 이로 인하여 정상사상의 위급도도 역시 감소될 것이다. 감소된 위기도의 량은 투입된 예산에 대한 효과의 척도를 제공할 것이다. 따라서 효과의 척도는 안전도 투자로서 추정될 수 있다.

4. FTA에서의 불확실성 분석 모델 개발

FTA에서 사용된 기본 사상의 매개변수 결정에 있어서 많은 실제적인 이유로 불확실성이 내포하게 된다. 그러므로 기본사상의 매개변수는 확률변수(random variable)로서 취급되기도 한다. 확률변수로 간주되는 정량적인 불확실성은 확률분포에 있어서 폭(spread)으로 추정될 수 있다[7,10].

가장 간단하고 해석적인 폭의 척도는 분산이므로 불확실성의 척도로는 분산이 적격이다. 고려되는 모델은 정상사상의 분산분할(variance partitioning)이 기본사상과 중간사상의 비선형 해석함수로서 나타내어 진다. 이와 같은 분할은 정상사상의 불확실성에 가장 큰 영향을 미치는 요소를 규정할 수 있어서, 그 요소 즉 기본사상과 중간사상들의 불확실성을 감소시키므로서 시스템의 불확실성을 배제하여 정상사상의 정확한 값을 도출해 낼 수 있다.

2차의 정상사상 함수를 고려해 보자.

정상사상의 확률 P는 다음과 같다[5].

$$P = a_0 + \sum_{i=1}^{m} a_i * P_i + \sum_{i=1}^{m} b_i * P_i^2 + \sum_{i<j} a_{ij} * P_i * P_j \quad \cdots\cdots \langle 8 \rangle$$

여기서 P_i는 시스템의 기본사상 즉 입력변수의 값이며, a_0, a_i, b_i, a_{ij}는 2차 출력 함수들의 계수이다. 위 식은 분산분할이 가능하며, 고정된 i에 대하여 1, P_i, P_i^2 값을 1, $P_i - p_i$, $P_i^2 - c_i * P_i - d$로 순서대로 대응 시켜서 P값을 다시쓰면 다음 식과 같다.

$$P = \bar{a}_0 + \sum_{i=1}^{m} \bar{a}_i * (P_i - P_i) + \sum_{i=1}^{m} \bar{b}i * (P_i^2 - c_i * P_i - d_i) + \sum_{i<j} \bar{a}_{ij} * (P_i - p_i) * (P_j - p_j) \quad \cdots\cdots \langle 9 \rangle$$

단, $\bar{a}_0 = a_0 + \sum_{i=1}^{m} [a_i * p_i + b_i * (c_i * p_i + d_i)] + \sum_{i<j} a_{ij} * p_i * P_j$

$\bar{a}_i = a_i + b_i * c_i + \sum_{j=i} a_{ij} * p_j$, $i = 1, 2, \cdots\cdots, m$

$\bar{b}_i = bi$, $i = 1, 2, \cdots\cdots, m$

$\bar{a}_{ij} = a_{ij}$, $1 < i < j < m$

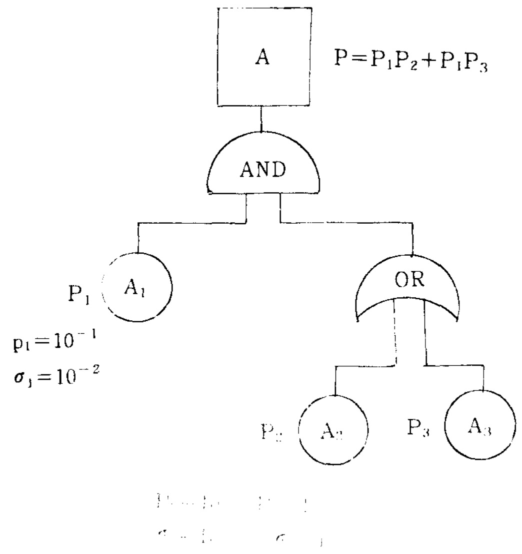
$p_i = E(P_i)$, $i = 1, 2, \cdots\cdots, m$

$\sigma_i^2 = \mathrm{Var}\{P_i\}$, $i = 1, 2, \cdots\cdots, m$

윗 식은 확률 변수 P_1, P_2, …, P_m이 서로 독립이고, 고정된 i에 대하여 대각선 순서대로 1, $P_i - p_i$, $P_i^2 - c_i * P_i - d_i$로 대응시키면 분산 분할은 다음 〈식 10〉과 같다.

$$\mathrm{Var}\{P\} = \sum_{i=1}^{m} \bar{a}_i^2 * \mathrm{Var}\{P_i\} + \sum_{i=1}^{m} \bar{b}_i^2 * \mathrm{Var}\{P_i^2 - c_i P_i\} + \sum_{i<j} \bar{a}_{ij}^2 * \mathrm{Var}\{P_i\} * \mathrm{var}\{P_j\} \quad \cdots\cdots \langle 10 \rangle$$

다음 〈그림 5〉의 FT로 예를 들어보자.



〈그림 5〉 FTA에 있어서 불확실성 모델 수치예

〈식 9〉 〈식 10〉에 의하여 정상사상의 2차 출력해수와 분산분할을 구하면 다음과 같다.

$$P = p_2(P_1-p_1)+p_1(P_2-p_2)+p_3(P_1-p_1)+p_1(P_3-p_3)+(P_1-p_1)*(P_2-p_2)+(P_1-p_1)*(P_3-p_3)$$

$$Var[P] = (p_2+p_3)^2 * \sigma_1^2 + p_1^2 * \sigma_2^2 + p_1^2 * \sigma_1^2 * \sigma_2^2 + \sigma_1^2 * \sigma_3^2 = 2.42\times10^{-5}$$

각 요소, 즉 기본사상과 중간사상의 정상사상 확률 P에 대한 기여율은 다음 〈표 3〉과 같다.

〈표 3〉 사상들의 기여율

사상	A_1	A_2	A_3	A_1 and A_2	A_1 and A_3	A_2 and A_3
기여율(%)	17	41	41	0.5	0.5	0.0

5. 결 론

FTA는 복잡한 산업안전 시스템의 신뢰도와 안전도를 결정하는데 이용되는 해석적 기법이다. 이를 이용하여 다양한 대체적인 안전 투자안을 분석하여서 산업안전 관리자가 안전을 위한 예산을 효과적으로 할당하기 위한 하나의 척도를 제공하는 것이며, 궁극적으로는 안전재해를 줄이는데 그 목적이 있다. 이로 인하여 기대되는 부수적인 효과로서는 산업안전 시스템에 대한 이해증진과 시스템의 고장원인을 체계적으로 파악할 수 있다. 또한 시스템의 잠재된 문제점이 제기됨으로써 신뢰성이 향상되며, FMEA(Failure Made Effect Analysis)의 보조수단으로서도 활용이 가능하다.

그리고, FTA분석에 개입되는 불확실성을 분석하는 해석적 모델을 제시함으로써 정상사상에 가장 큰 영향을 미치는 요소 즉 기본사상이나 중간사상을 규정할 수가 있다. 이들의 불확실성을 감소 시킴으로써 시스템 전체의 불확실성 요인을 배제하여 정확한 정상사상의 값을 계산할 수가 있다.

참고문헌

1. 박철수 산업안전관리론, 중앙경제사, 서울, 1989.
2. 신승현, 인간공학, 형설출판사, 서울, 1985.
3. 이근희, 안전관리학, 창지사, 서울, 1987.
4. 이근히, 이동형, "Fault Tree Analysis을 활용한 집진기(Bag Filter) 고장의 체계적 분석," 공업경영학회지, 제12권, 제20집, 1989.
5. Ali M. Rushdi, "Uncertainty Analysis of Fault-Tree Outputs," *IEEE Trans Reliability*, Vol. R-34, No. 5, pp. 458-462, 1985.
6. David B. Brown, *Systems Analysis and Design for Saftey*, Prentice-Hall, Inc., 1976.
7. David C. Cox, "An Analytic Method for Uncertainty Analysis of Nonlinear Output Functions, with Applications to Fault-Tree Analysis," *IEEE Trans. Reliability*, Vol. R-31, No. 5, pp. 465-468, 1982.
8. Hideo Tanaka, et al, "Fault Tree Analysis by Fuzzy Probability," *IEEE Trans. Reliability*, Vol. R-32, No. 5, pp. 453-457, 1983.
9. J. R. Taylor, "An Algorithm for Fault Tree Construction," *IEEE Trans. Reliability*, Vol. R-31, No. 2, pp. 137-146, 1982.
10. Marcelo Masera, "Uncertainty Propagation in Fault Tree Analysis Using Lognormal Distributions," *IEEE Trans. Reliability*, Vol. R-36, No. 1, pp. 145-149, 1987.
11. Thomas Feo, "PAFT F77, Program for the Analysis of Fault Trees," *IEEE Trans. Reliability*, Vol. R − 35, No. 1, pp. 48-50, 1986.
12. W. S. Lee, et al, "Fault Tree Analysis, Methods and Applications," *IEEE Trans. Reliability*, Vol. R-34, No. 3, pp. 194-203, 1995.