《技術解說》

Journal of the Human Engineering Society of Korea
Vol. 1 No. 1 June 1982

Fault-Tree를 이용한 안전사고의 체계적 분석

(Systematic Analysis of Accidents by Fault-Tree)

李 相 遠†

안정성의 관점에서 씨스템을 분석 평가할 때에 다음과 같은 3가지 접근 방법이 있을 수 있다.

첫째, 과거의 경험에 의한 것으로서 "어떤 일은 하면 안된다(Don't Do's)"라는 점검표(Checklist)를 사용하는 직관적인 방법.

둘째, "어떤 일이 발생하였을 때 어떻게 처리하여야 안전한가? (the HOW to the WHAT HAPPENED)"의 귀납적인 방법.

셋째, 어떻게 하여 무슨일이 발생할 것인가? (the WHAT HAPPENED to the HOW) 의 연역적인 방법이다.

System의 안정성을 평가 분석하는 데에는 세번째의 연역적인 방법이 가장 좋으며 이 연역적인 여러 기법들 중에서 가장 일반적인 방법이 "Fault Tree Analysis"란 기법으로 알려져 있다. 여기에서는 Fault-Tree를 이용한 대안들을 평가하는 것에 주안점을 두기로 한다.

Fault Tree 분석 기법의 개요

Fault Tree 분석 기법은 복잡한 System의 신뢰성과 안정성을 평가 분석 하는데에 매우 유효한 기법으로 등장하고 있으며 1962년 Bell 전화 연구소의 H. A. Watson이 Minuteman 발사 조정 씨스템의 안정성 평가를 위하여 이 개념을 처음으로 실제 적용하였으며 그 후에 항공학, 원자력공학등 여러 분야에서 적용 하였다[1, 2]

Fault-Tree란 씨스템의 고장요인들의 관계를 Boolean logic gate를 이용하여 도해적으로 표시한 cycle이 없는 oriented, connected된 graph이며 flow는 각 기초 고장들의 확률이 된다.

Fault-Tree의 용어 및 가정

Fault Tree를 작성하기 위하여 다음과 같은 용어, 기호 및 가정을 이해 하여야 한다.

A. 용 어

1. event : 분석하려는 system 내에서 발생하는 사건들로서 그 수준은 단위부품, subsystem, system이 될 수 있다.

2. Basic event : system을 구성하는 기본 단위의 고장을 의미하며 분석하려는 의도에 따라 basic event는 기본 단위의 조합인 subsystem이 될 수도 있다. 또한 부품 자체의 특성으로 인하여 발생하는 event를 primary event 라고 하며(예 : 전구의 필라멘트가 노후화 하여 끊어짐) 외부의 원인으로 인하여 발생하는 event를 secondary event(예 : 과도전류로 인하여 끊어짐)라고 분류한다.

3. Top event : 분석하려는 system 자체의 고장을 의미한다.

B. 기 호

Fault-Tree에 사용되어 지는 기호는 표 1과 같다.

C. 가 정

Fault tree 분석시의 가정은 다음과 같다.

(1) 부품이나 subsytem은 작동과 부작동의 두가지 상태로만 존재한다.

(2) 각각의 고장은 서로 독립적이다.

(3) 각 부품 고장은 exponential의 분포를 갖으며 일정한 고장율을 갖는다.

†空軍本部 体系分析室

표 - 1 Fault-tree 작성에 사용되는 기호

종 류	명 칭	기 호	의 미
Logic 기 호	AND gate		모든 input이 true 일때 output이 true가 된다.
	OR gate		한개 또는 한개 이상의 input이 true이면 output이 true가 된다.
Event 기 호	Rectangle		좀더 세밀히 고장을 분석해야 함.
	Circle		주어진 씨스템의 기초고장 (basic event)
	Diamond		더 분석 가능하나 basic event로 가정
	Transfer out		다른 gate로 나가는 event
	Transfer in		다른 gate로 부터 들어오는 event

가정 (1), (2)는 Boolean logic을 적용하기 위한 것이나 실제 상황에서는 부분적으로 생기는 고장으로 인하여 전체 씨스템의 성능이 저하만 되는 경우도 존재한다.

Fault Tree의 작성

일반적으로 작성 절차는 다음과 같다.

(1) 분석하려는 씨스템을 정의한다. 이때 분석 대상의 범위를 잘 선택하여야 하며 너무 광범위하게 잡으면(예 : 항공기 추락) 분석에 어려움이 따르게 되며 너무 좁게 잡으면(예 : 변개구름 속을 비행중 날개가 손실되어 추락) 씨스템을 충분히 분석할 수 없는 경우도 존재 한다.

(2) Top event의 원인이 되는 basic event (primary, secondary event)를 분석한다.

(3) Top event와 basic event의 관계를 Boolean logic gate를 이용하여 도해한다.

(4) (2), (3)단계에서 결정된 event가 더 세분이 가능한지 분석한다. 세분 가능하면 그단계에서 구한 event를 top event로 하여 (2), (3) 단계를 되풀이 하여 더 이상의 분석이 필요 없을 때까지 계속한다.

(5) Fault-Tree를 간략화 한다.

(6) 정성, 정량 분석을 한다.

이상과 같은 단계로 Fault-Tree를 분석하며 이때에 발생될수 있는 오류는 다음과 같다

(1) 씨스템은 잘못 이해하거나 생략한다.

(2) 부정확한 data를 쓰거나 아주 복잡한 씨스템에서는 분석의 수준을 잘못 정한다.

(3) 동일 Fault-Tree에서 나타나는 상호 배제적인 event를 잘못 계산한다.

Fault tree의 용도

Fault-Tree는 다음과 같은 여러가지의 정성, 정량 분석을 하는데 쓰여진다.

(1) Minimal cut set을 이용하여 system의 reliability, structural ordering, probability ordering을 구하여 씨스템의 안전도에 대한 파악을 할 수 있다. (4) Cut set이란 top event를 유발시키는 basic event의 intersection으로 표시되어 진다. Cut set중 중복되어 지는 부분을 제거한 후 남는 set을 minimal cut set의 union으로 표시된다. minimal cut set을 구하는 방법은 두가지로 분류될 수 있다. 즉 Bottom up approach, Top down approach 의 접근 방법 이다. 자세한 방법은 Reference 를 참고하기 바란다.

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

(3) 씨스템의 고장난 부분을 쉽게 찾을 수 있다.

(4) 씨스템의 설계 변경에 관심이 적은 경영진에게 system을 도해적으로 보여 줄 수 있다.

(5) 분석자가 하나의 씨스템에 집중적으로 고장 탐구를 할 수 있다.

(6) 분석자가 System의 behavior를 면밀히 조사할 수 있다.

다음에는 씨스템의 안전 개선을 위한 대안 선택을 Fault-Tree를 이용 분석하여 보자.

금강석을 가공중 부스러기가 눈에 들어가는 사고가 발생하므로 이 사고를 방지하기 위하여 여러 대안들을 Fault Tree를 이용하여 비용/효과 분석 경우를 보자. 이때의 Fault Tree는 그림 1 과 같으며 확율을 넣어 간략화한 것은

그림 2 와 같다. 여기서 확율이라 함은 단위 시간당 사고 발생수이다. 과거의 기록에서 볼 때 사고의 유형은 표 2 와 같으며 사고 발생은 first aid 7, temporary total 2, permanent partial 1건 이었다.

Table2 Example of negative utility schedule

Severity Classification	*Severity*	*Money*
1	First Aid	20
2	Temporary Total	345
3	Permanent Partial	2,500
4	Permanent Total (including fatalities)	21,000

그러므로 사고 발생시 비용의 기대값은

$E=(0.7)(20)+(0.2)(345)+(0.1)(2500)=333$

OR gate인 경우 어느 event가 발생 하여도 되므로 OR gate가 발생할 확율은

$P_{OR}=1-\pi_{i=1}^{n}(1-q_i)$가 된다.

AND gate인 경우 모든 event가 동시에 발생하여야 함으로 발생할 확율은

$P_{AND}=\pi_{i=1}^{n} q_i$가 된다. 여기서 q_i는 event i가발생할 확율이다. 윗 식을 사용하면 event C, event E가 발생할 확율은

$P_E=1-(1-0.05)(1-0.05)(1-0.01)$
$=0.1065$

$P_C=(0.8)(0.1065)(1)(0.5)=0.0426$이 되고 Top event A가 발생할 확율은

$P_A=1-(1-0.01)(1-0.0426)=0.0522$ 가 된다. 그러므로 Top event A에 대한 기대 비용은

$C=P_A \cdot E=(0.0522)(333)=1738$ 이 된다. 이 씨스템의 안전을 개선키 위하여 표-2와 같은 대안들이 있다.

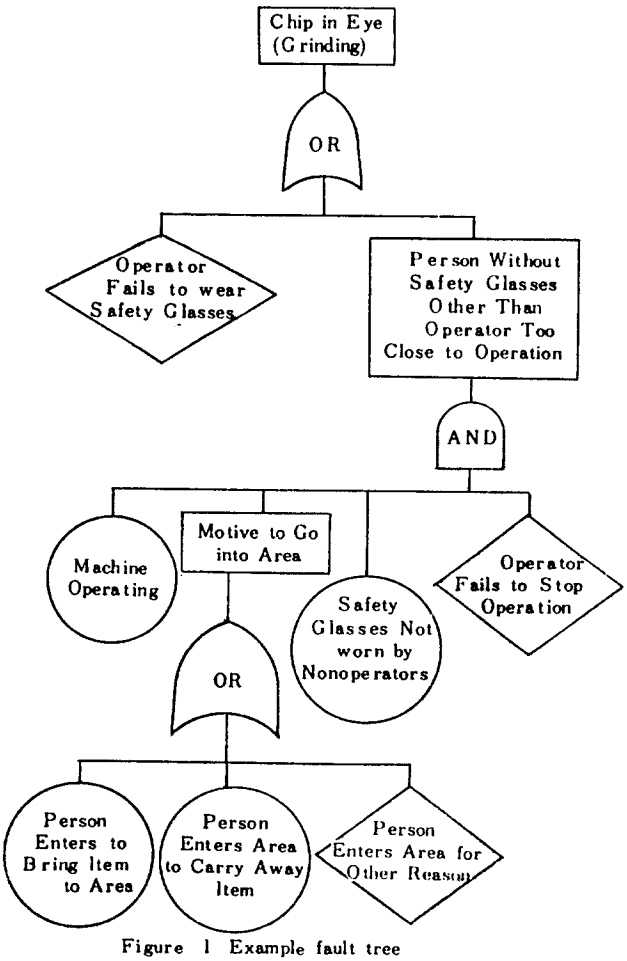

Figure 1 Example fault tree

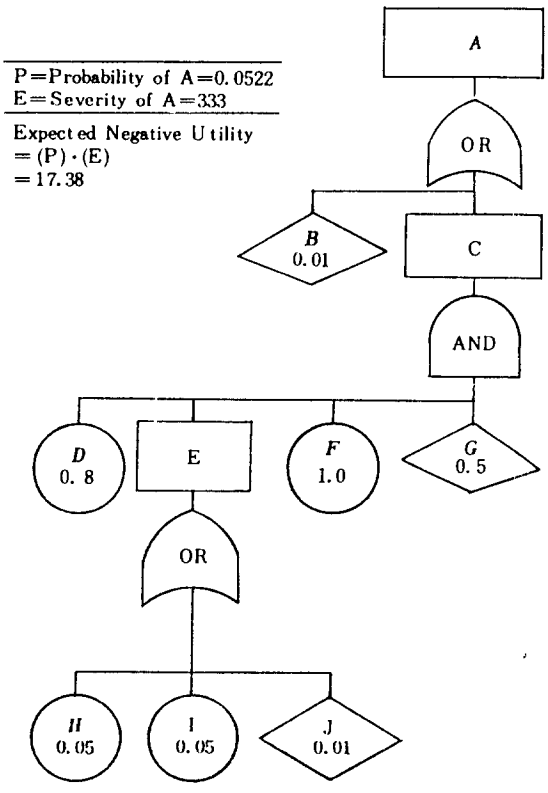

Figure 2 Example fault tree with probabilities assigned

Table3 Alternatives for example

Alternative	Description	Prorated Cost/mmh	Effect
1	Ensure that operator stops operation whenever anyone enters area	$25	Reduce probability of event G to. 05
2	Move storage area away from grinding area	$15	Reduce probability of events H and I to zero
3	Both 1 and 2	$30	Same effects as both 1 and 2

Table4 Summary of alternatives for example

Alternative	Cost	Original Criticality	New Criticality	Benefit	Cost/Benefit
1	$25	17.38	4.73	12.65	1.98
2	$15	17.38	4.65	12.73	1.18
3	$30	17.38	3.46	13.92	2.16

각각의 대안들에 대하여 앞의 방법으로 기대 비용을 분석하고 평가하면 표 3과 같다.

표 3에서 볼때 대안 2가 비용/효과면에서 최선의 방안이 된다. 그러나 실제 대안의 선택은 가용금액의 수준에 따라 각 대안들이 비교 선택 되어지며 또 다른 투자 대상이 있다면 다른 투자 대상과의 한계(marginal) 비용/효과 면에서 비교하여 투자가 이루어 진다.

맺는 말

기계, 인간, 재료의 각개 또는 혼합 씨스템에서 발생하는 안전 사고의 분석에 있어서 Fault-Tree는 매우 유효한 기법이다. Fault Tree는 Hardware 뿐만 아니라 Soft ware 에인 것, 인간-기계 씨스템의 안전 분석에 사용될 수 있다. 여기서는 안전 사고 방지를 위한 투자시 대안 선택에 있어서 우선 순위를 정할 수 있는 정량적인 방법을 Fault Tree를 이용하여 비용/효과 면에서 평가 할 수 있는 방법을 제시 하였다. 안전을 위한 대안 선택도 투자하려는 예산의 정도에 따라 많이 변경될 수 있다.

Fault-Tree 분석이 안전 평가를 위한 좋은 방법이지만 복잡한 씨스템에서는 개발시 비용이 많이 들고 Fault-Tree를 만드는 자체가 매우 지루하며 씨스템을 이해하기 위해서는 여러명의 전문가가 모여야 한다는 단점도 존재한다. 또한 앞에서 언급한 바와 같이 여러가지 가정이 실제와 부합되지 않는 경우도 많이 존재하게 되며 Cut set을 이용한 분석을 할 때에는 Computer의 도움 없이는 거의 불가한 경우도 존재한다.

참 고 문 헌

[1] Recht. J. L., "System Safety analysis:The fault tree", *National safety news*, Apr. 1966.

[2] Crosetti, P. A., "Commercial application of fault tree analysis" in *Proc. Reliability and Maintainabity conf. vol 9*, 1970, pp. 230-244.

[3] Fussell, J. B., Power, G. J., Bennetts, R. G. "Fault tree-A state of the art discussion", *IEEE Trans, Rel.* Vol. R-23 No. 1, Apr, 1974

[4] Barlow, R. E., Proschan, F., *Statistical Theory of Reliability and life testing*, N. Y. :Holt, Rinehart and Winston, INC. (1975)