解　說

Fault Tree Analysis 의概要

高　南　俊

學會常任研究委員

1. 序　論

1－1. System 安全工學

지금까지의 安全을 한마디로 말하면 要素安全 즉 機械, 機具, 設備, 作業方法등 필요한 要素別로 安全對策을 생각해 왔다. 이에 대하여 System安全이라고 하면 機械마다의 工程이 綜合된 全 工程 즉 System全體에 대한 綜合的 安全을 System安全이라고 말할 수 있다.

A 工程에서의 缺陷이 事故없이 B 工程으로 흘러가서 事故를 유발할 수도 있고 혹은 C 工程에서 災害를 發生시킬 수도 있으며 그 事故가 當該工程으로 끝나는 것이 아니라 全工程을 마비 시키거나 破괴 시키는 結果를 초래 하게 되므로 從來의 方式에 따른 缺陷工程에 局限된 安全만으로는 設備의 安全性을 確保할 수가 없는 것이다.

여기서 잠시 System安全의 歷史를 살펴보지 않을 수 없다.

元來 System安全은 1950年代 후반 東西간의 軍備경쟁의 와중에서 開發되기 시작한 미사일 開發作業에서 연속 4回의 大事故가 發生하여 수 100萬$의 損失을 가져 왔다.

이때 그 原因調査 결과 根本的으로 해결하지 않으면 안될 安全性에 관한 몇가지 문제가 지적되기에 이르러 1962年 「空軍彈道 미사일開發을 위한 System安全工學」이라는 最初의 美軍사양서가 公表되고 이후 이 System Safety는 全 美軍에 적용되면서 1977年 6月 MIL-S-882 A 「System 安全計劃의 必須條件」(System Safety Program Reguirement)이 되어 오늘에 이르고 있다. 元來이 規格은 美軍의 裝備에 關한 계약 條件으로 制定되었으나 現在는 一般產業에 있어서의 System 安全에 關한 有力한 지침으로 활용되고 있다.

이와 함께 1974年 美原子力 委員會가 실시한 原子力 플렌트 安全評價에서도 이러한 System 技法이 적용되어 System安全工學의 發展에 크게 기여하게 되었다. 日本國에서는 1976年 勞動省에서 化學플렌트의 安全性評價에서 F.T.A에 의한 再評價를 실시하여 System安全分析 技法이 全國으로 확산 오늘에 이르고 있다. 本章에서는 System安全工學의 한 解析技法인 F.T.A(Fault Tree Analysis)에 關해서 그 基本的인

事項을 論하고 運用에 關해서는 다음에 論하기로 하겠다.

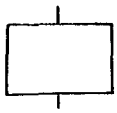
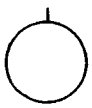
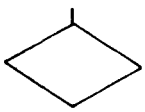
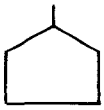
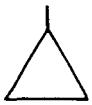
1 - 2. F.T.A의 槪要

F.T.A는 機械, 設備 또는 man-machin system의 고장이나 災害의 發生要因을 論理的 圖表에 의하여 解析하는 方法으로서 故障이나 災害要因의 定性的인 색출뿐만 아니라 개개의 要因이 發生하는 確率을 얻을 수가 있다. 그러나 論理的 限界性이 없는 것은 아니며 特히 定量的 解析에 있어서 어려움이 있기도 하다.

무엇보다도 重要한 것은 災害發生後의 原因규명보다 災害發生 以前에 豫測技法으로서의 活用가치가 높다는 事實이다.

F.T.A는 다음과 같은 일정의 約束된 記號에 의하여 각각 그 뜻을 나타내고 論理的 순서에 따라 展開하여 나가며 더 이상 論理的 전개가 안될때까지 追求해 가는 것이다. 그러기 위하여 여기에 사용되는 다음과 같은 統一된 記號를 사용하게 되며 이 記號는 각각 獨立된 意味를 안고 있다.(표1 참조)

表1. FTA에 사용되는 논리기호(기본형)

No.	기 호	명 칭	설 명	
1		결 함 사 상	개별적인 결함사상	
2		기 본 사 상	더 이상 전개되지 않는 기본적인 사상 또는 발생확율이 단독으로 얻어지는 낮은 레벨의 기본적인 사상	末端事象
3		이 하 생 략 (최후사상)	정보부족 해석기술의 불충분등으로 이상 더 전개할 수 없는 사상 작업진행에 따라 해석이 가능할 때는 다시 속행한다.	
4		통 상 사 상	통상 발생이 예상되는 사상(예상되는 원인)	
5	 (IN)	이 행 기 호	F.T. 도상에서 다른 부분에의 이행 또는 연결을 나타냄. 삼각형 정상의 선은 정보의 정입 루-트를 뜻한다.	
5'	 (OUT)	이 행 기 호	5와 같다. 삼각형의 옆의 선은 정보의 전출을 뜻한다.	
6	출력  입력	「AND」게이트	모든 입력사상이 공존할 때만이 출력사상이 발생한다.	

7	출력 입력	「OR」 게이트	입력사상중 어느것이나 하나가 존재할 때 출력사상이 발생한다.
8	출력 조건 입력	제약게이트 (제지게이트)	입력사상에 대해서 이 게이트로 나타내는 조건이 만족하는 경우에만 출력사상이 발생한다. 조건부확율

2. F T.A의 해석절차

2 - 1. FTA 의 규제사항

그림은 발판에서의 추락재해의 FTA이다. 이 그림에서 보는바와 같이 FTA 는 여러가지 현상을 정해진 기호의 상호연결로 그 의미하는 바를 논리적으로 전개해 나간다.

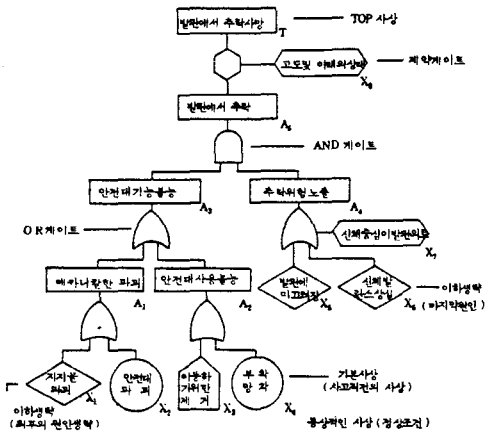


그림 1. 발판에서의 추락재해에 대한 FTA

F.T.A 는 그의 이론적인 전개를 어떤 기호로서 시행하는 것이다.

그 기호는 고유의 뜻을 지니고 있으며 논리적으로 사용되도록 규제하고 있다. 그러나 FTA 는 비교적 새로운 기법으로 그 기호는 아직도 몇가지 문제를 안고 있다. 원래는 정보교환의 도구로서 제 3자의 도움없이도 기호만을 보고 이해 될 수 있어야만 하는 것이다.

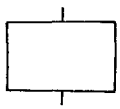
F.T.A 는 한마디로 논리적인 해석도표라고 할 수 있다. 어떤 해석하고자 하는 현상을 정점에 표시해 놓고 거기서부터 그러한 현상이 어떻게 일어나는가를 순서대로 질문하여 추구하면서 그 원인들이 나무가지로 서로 어떤 연관성을 가지고 작용하는 가를 기호를 통하여 추리해 가면서 궁극적 지점에 도달하게 된다.

이러한 현상을 나타내는 기호는 2가지 종류가 있다. 하나는 현상을 나타내는 기호이며 다른 하나는 현상을 연결하는 논리게이트 이다.

논리게이트란 현상간의 연결통로라 할 수 있다. 통상 원인이 되는 현상간의 통로의출입문으로 되어 있다.

2 - 2. 기호의 종류

(1) 결함현상 〈기호〉 4각의 틀

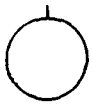


결함이 재해로 연결하는 현상 또는 사실 상황등을 나타내고 논리게이트의 입력 또는 출력이 된다. 결함이냐 아니냐의 양자택일로 표시되며 중간은 없다.

F T도표의 정상에 설정되는 사상 즉 이제부터 해석하고자 하는 사상을 특히 톱사상이라

부르며 치명적 사고등이다. 이 사상을 기호로 표시한다.

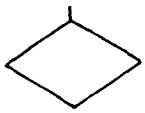
(2) 기본현상 〈기호〉 원형



더 이상 추적할 수 없는 궁극적인사상 항상 논리게이트에의 입력이며 출력은 되지 않는다. 예를 들면 스위치 접점불량스파크, 타이어의 펑크등은 기본사상이다.

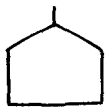
그러나 어떤 사상이 기본사상이냐 아니냐의 기준은 명확하지가 않다. 오히려 케이스바이 케이스로 정하는 것이 옳다. 통상 조작미스나 착오등의 휴먼에라는 기본사상으로 취급된다.

(3) 추적불가능한최후사상 〈기호〉 다이어몬드 형



정보부족 해석기술의 더이상 원인 분석이 곤난한 최후적사상

(4) 통상사상 〈기호〉 지붕형



결함사상이 아니라 발생이 예상되는 사상, 예를들면 기상조건이나 환경조건등 화재발생시 공기의 존재라든가 또는 기계등의 조작순서 등의 기호는 더 이상의 발전이 없으며 대부분이 한가지로 끝난다.

(5) 말단사상 나무가지의 끝, 기본사상, 추적불가능한 최후사상, 통상사상의 총칭

2 - 3. 이행기호

이행기호 〈기호〉 삼각형

(IN)

(OUT)

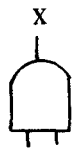
같은 FT그림안의 다른부분과 같을 경우 반복을 생략하기 위하여 거기에 이행하는것을 나타내기 위해 사용하나그림을 한장안에다 써 넣을 수 없을때 나무의 이음을 나타낼때 사용하기도 한다.

IN의 방향은 전입을 OUT의 방향은 전출을 통상 어디서 어디까지 이행하는가를식별하기 위해 과 같이 대응하는 in과 out 의 삼각형안에 문자 또는 수자를 써 넣는다.

2-4. 논리게이트

사상간의 인과관계를 표현하는 것이 논리게이트다. FTA의 중심적 특징의 하나다.

(1) ANDgate 출력x의 사상은, A, B 모든 사상이 동시에 존재할 때 발생하며 A, B 어느 한 쪽만의 존재로는 발생하지 않는것을 나타내는 게이트이다. 이 기호는 AND 또는 · 와같이 표시 될 때도 있다.



예를들면 그림 2에서 렘프에 불이켜 지지 않는 사상이 발생하기 위해서는 A,B,C의 스위치가 전부 off 가 되어야 한다 이때 톱 사상인 「불켜지지 않음」 이 ABC 의 스위치 off 라는 기본사상과 연결시키기 위해서는 이 논리게이트가 있어야만 하는 것이다.

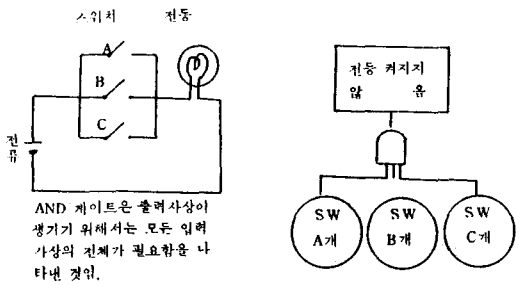
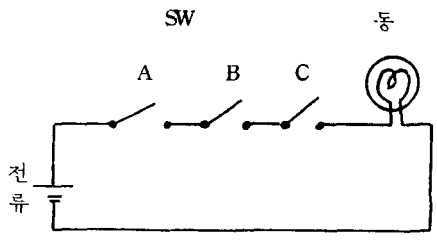


그림 2. AND 게이트

(2) OR게이트 출력x의 사상은 A, B의 어느것이나 한가지 또는 그 구성이 (어떤것이든 무방) 존재할 때 발생하는 것임을 나타내는 게이트이다.

이 기호는  또는  와 같이 표시되는 경우가 많다.

예를들어 그림 3에서 「불이 켜지지 않음」이라고 하는 사상이 발생하기 위해서는 A, B, C의 스위치 중 어느것이나 하나가 off 가 되면 되는 것이므로 입력사상과 출력사상을 연결하는 논리게이트는 OR게이트라야만 한다.



OR게이트는 만약 역사상의 어느것이나 일어난다면 출력 사상도 일어난다고 하는 것을 나타낸다.

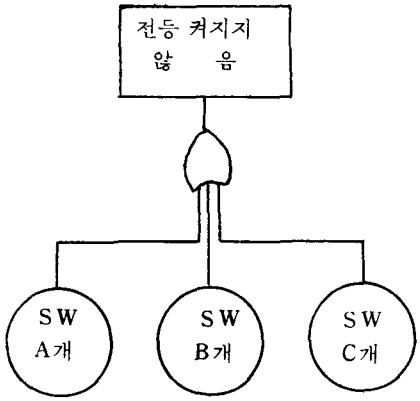


그림 3. OR게이트

또한 그림1의 안전대가 가능상실이라는 A_3의 사상은 안전대의 "메카니칼한 파괴"를 나타내는 A_1의 사상이, "안전대를 사용불능"의 A_2의 사상중 어느것이든 하나의 사상만으로 발생하므로 OR게이트로 연결되고 있다.

(3) 제약게이트 (제지게이트) 이 게이트는 입력사상이 생김과 동시에 어떤 조건을 나타내는 사상이 발생할때 만이 출력사상이 생기는 것을 나타냄 좌측 그림의 경우 A의 사상이 존재하고 또한 C의 조건사상이 만족하면 비로서 출력사상 x가 발생한다.

그림 1에도 이제약게이트가 사용되고 있으나 발판에서의 추락이라고 하는 A_5의 사상이 존재하고 그 발판의 "고도 및 아래 상태"라고 하는 조건 X_8이 일정높이 이상으로 높고 아래가 콘크리트라고하는 조건이 충족되어 비로서

Top 사상인 발판에서의 추락 사망이 발생한다는 것을 나타내고 있다.

또한 그림의 C는 조건記號(修正記號) 라고 불리워 지고 있으나 ⬭ 形으로 사용될 때도 있다.

또한 그림 1에서의 X_7 도 條件記號이며 否定的 展開事象이 되고 있는 X_5 「발판위에서 미끄러짐」 및 X_6 인 「身體의 균형상실」 가운데 어느것이나 1개가 발생했을때 반듯이 出力事象 A_4 「추락하고 있다」는 事象이 생기는 것이 아니라 「身體의 重心이 발판 밖으로 기운다」라는 條件이 前提할때만이 생기는 것을 뜻하고 있다.

條件記號는 이와같이 論理 Gate에 가중해서 사용되기도 한다.

3. F.T.A 의 作成절차

3-1. F.T.A 의 産業安全에의 活用

System安全에서 탄생한 F.T.A는 災害結果에서 부터 그 原因규명의 한 分析技法으로 탄생하였으나 그후 오늘에 이르러서는 災害結果가 아닌 豫測工學으로서 設計와 制造단계서 그 危險의 可能性 여부를 Check 하는 管理技法으로 運用되기에 이르렀으나 컴퓨터, 로봇트의 登場은 F.T.A 의 活用과 發展을 촉진한 것이다.

F.T.A 의 作成時機는 다음 3가지로 나누어 볼 수가 있다.

첫째는 災害가 發生했을때이며

둘째는 機械設備를 設置가동할 때

셋째는 危險내지는 故障의 우려가 있거나 그러한 事由가 發生했을 때이다.

그러나 최근에는 수시로 安全評價를 하는데 사용되고 있다.

作成에 앞서 생각할 것은 目的이 分明해야하며 충분한 資料를 준비해야 한다. 다음에 간단한 추락災害의 作成의 例를 제시해 본다.(그림 4).

그림 4는 추락災害가 發生한 후 原因 규명을 目的으로 F.T.A을 적용한 것이다.

굵은 線에 제시된 事象이 末端要因으로 災害가 발생하였다면 굵은線의 部分的 解析만으로 끝나는 것이다.

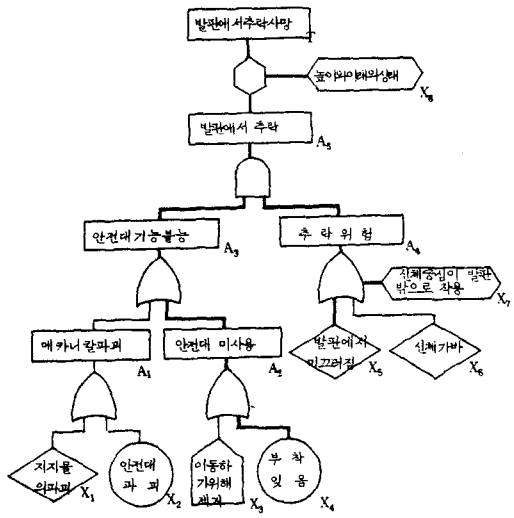


그림4. 발판에서의 추락재해의 F.T.A.

3-2. F.T.A 의 절차

F.T.A 의 절차는 그 목적과 해석의 精密度에 따라 다르나 통상적으로 다음의 3단계로 나누게 되는 경우가 많다.

1) 定性的 F.T(Fault tree)의 작성단계

分析하고자 하는 재해를 결정하고 이것을 F.T에 나타내기 까지의 단계로 그것을 상세하게 다음과 같이 나타낸다.

① 分析하고자하는 System의 공정과 작업내용을 충분히 파악한다.

② 예상되는 재해를 과거의 재해사례와 재해통계를 기초로 될 수 있으면 광범위하게 조사한다.

③ 재해의 강도, 빈도, 시스템에 미치는 영

향등을 검토하고 해석의 대상이 되는 재해를결정한다.

④ 재해에 관계되는 기계등의 불량상태와 작업자의 error에 대해 그 원인과 영향을 될수 있으면 상세히 조사한다. 이를 위해 필요가 있으면 예비적 해석을 행한다.

⑤ F,T를 작성한다.

2) F,T의 定量化 단계

1)에서 작성한 FT를 數式化하고 재해의 발생確率을 計算하는 단계이다.

① 해석하는 災害 發生確率의 目標値를 危險度, 동종(同種)시스템의 數, 外部에의 영향등을 고려해서 정한다.

② 작성된 FT를 수식화하고 부울代數를이용해서 간소화한다.

③ 災害原因이 되는 기계등의 不良狀態와 작업자의 error發生확률을 調査와 資料에 의해구한다.

④ ③의 값을 수식화된 FT에 대하여 재해의 발생확률을 계산한다. 〈계 속〉

科學技術人의 信條

우리 科學技術人은 科學技術의 暢達과 振興을 通하여 國家發展과 人類福祉社會가 이룩될 수 있음을 確信하고 다음과 같이 다짐한다.

一. 우리는 創造의 精神으로 眞理를 探究하고 技術을 革新함으로써 國家發展에 積極寄與한다.

一. 우리는 奉士하는 姿勢로 科學技術 振興의 風土를 造成함으로써 온 國民의 科學的 精神을 振作한다.

一. 우리는 높은 理想을 指向하여 自我를 確立하고 相互協力함으로써 우리의 社會的 地位와 權益을 伸張한다.

一. 우리는 人間의 尊嚴性이 崇尙되고 그 價値가 保障되는 福祉社會의 具現에 獻身한다.

一. 우리는 科學技術을 善用함으로써 人類의 繁榮과 世界의 平和에 貢獻한다.