Fault Tree Analysis (결함수분석법)

1.1 개요

결함수분석법(FTA; Fault Tree Analysis)은 시스템 안전공학의 대표적인 방법으로서 1962년 미국 벨 연구소에 의해 처음으로 고안되었다.

이 방법은 미사일 발사 제어시스템에서의 우발사고를 예측하는 문제 해결방법으로서 이용되다가 보잉사에 의해 컴퓨터를 사용하는 시뮬레이션이 가능하도록 수정하는 등, 주로 보잉사를 중심으로 하는 항공 우주산업과 원자력산업을 시작으로 기타의 산업안전 분야에 적용할 수 있음이 인식되어 1965년부터 산업안전분야에 소개되었다.

일본의 경우는 일반산업 특히 화학공업 방면에서 FTA에 대한 관심이 지금과 같이 증진된 것은 1973년경의 연쇄폭발 누출 등의 재해를 계기로 해서 장치산업 등의 재해방지에 시스템안전적인 해석방법이 주어져서 재해의 예측이나 안전성의 사전평가의 필요성이 통감되었기 때문이다. 그러나 FTA에 관한 세계적인 관심을 일거에 높인 것은 1974년 미국 원자력위원회가 행한 상업용 원자력 플랜트의 위험성 평가 즉, '라스무센 보고(Rasmussen Report)'라고 불리우는 것으로 이 보고서 속에서 FTA가 대규모로 활용되어 재해의 예측이 이루어졌다.

라스무센 보고서의 내용은 100개소의 원자력 발전소에서의 재해발생빈도와 사망자수의 추정에 대한 것으로서 여기에 사용된 각종 설비·부품에 대한 신뢰도 및 고장률은 매우 방대하고 정밀한 분석과 검증절차를 걸친 자료로서 FTA수행에 좋은 참고자료로 활용되고 있다.

1962년 미국의 벨 전화 연구소에서 군용(minuteman launch control system) 목적의 안전성 평가에서 개발됨.

1965년 Mearns(벨 전화 연구소), Haasl, Feutz(보잉 사) 등이 symposium에서 발표.

1774년 Fussel, Powers, Bennetts 가 FTA의 장·단점에 대해 발표.

1976년 Fussel에 의해 FTA에 대한 General account가 이루어짐.

대기 우주 산업에서 시작 > 원자력 산업에 도입 > 화학 플랜트에 확산

1.2 정의

1.2.1 FT(Fault Tree) 정의

A **Graphical representation** of the interrelationships between equipment failures and a specific accident.

A **logic diagram** showing how initiating events, at the bottom of the tree, through a sequence of intermediate events, can lead to a top event.

A **deductive method** for idenfitying ways in which hazards can lead to accident.

Is designed by setting down the undesired event at the top and determining all the specific events which can bring about the failure.

Used to perform **quantitative calculations** to determine the **probability** of the top event.

Events in a fault tree are not restricted to handle failures. It can also include **software, human and environmental factors.**

1.2.2 FTA(Fault Tree Analysis) 정의

화학 플랜트, 핵 발전소, 대기 우주산업 및 전자공업에서 화재·폭발·누출 등 어떤 특정한 예상 사고에 대하여 그 사고의 원인이 되는 장치/ 기기의 결함이나 설계자/ 조업자의 오류를 연역적·순차적·도식적·확률적으로 검토 분석하여 이의 정성적·정량적 안전성을 평가 진단하는 방법.

A **deductive technique** that focuses on one particular accident event and provides a method for determining causes of that accident event.

A tool along with **component failure rate data and human reliability data** to determine how often such an event can occur.

A method for representing the **logical combinations** of various system states which lead to a particular outcome (**top event**).

A method frequently used as a **qualitative and quantitative evaluation** in order to assist the **designer, planner or operator** in deciding how a system may fail and what remedies may be used to overcome the causes of failure.

An analysis tool that used deductive reasoning and graphical diagrams showing the logic of the deductive reasoning process to deterine how a particular undesired event can occur.

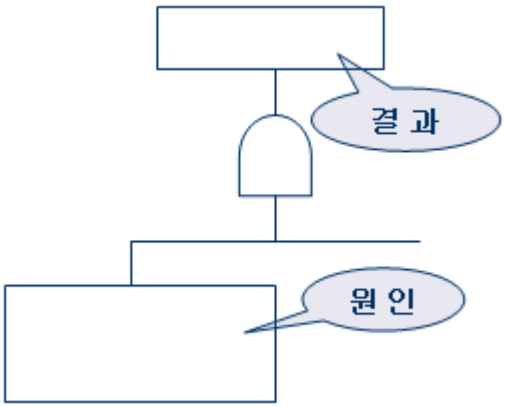
A deductive method which is normally used in a quantitative way, although it requires as an initial step a qualitative study of the system under consideration, just as any method of system analysis.

Permits the hazardous incident (top envet) frequency to be estimated from a logic model of the failure mechanisms of a system.

The model is based on the combinations of failure of more basic system components, safety systems, and human reliability.

1.3 특징

FTA는 시스템고장을 발생시키는 원인들과의 관계를 논리적으로 사용하여 나뭇가지 모양의 그림(Tree)으로 나타낸 FT(Fault Tree)를 만들고 이에 의거하여 시스템의 고장확률을 구함으로서 취약 부분을 찾아내어 시스템의 신뢰도를 개선하는 정량적 고장해석 및 신뢰성 평가 방법이다.



FTA의 가장 큰 특징은 AND와 OR인 두 종류의 논리게이트 조합에 의해 대상 설비 또는 공정의 위험성을 트리구조에 의해 표현하므로, 시각적으로 파악하는 우수한 수단이며 여러가지 전문 기술분야에 걸친 정보를 망라할 수 있는 유연성이 풍부한 방법이라고 할 수 있다.

또한 분석대상의 위험성에 대한 확률론적인 정량평가가 가능하게 하여 기본사상(Basic Event) 발생률로써 중간 및 정상 사상에 대한 확률을 차례로 계산할 수 있게 함으로서 기존의 감각적, 경험적 사고로부터 탈피하여 논리적이고 확률론적인 정량적 결과를 도출할 수 있게 하였다.

1.4 수행절차

시스템 안전도 분석을 위한 FT절차는 해석대상 시스템의 특성이나 목적, 수준에 따라 다소 차이가 있을 수 있으나 일반적으로 다음과 같다.

1.4.1 FTA 수행을 위한 준비사항

A complete process understanding

Information from FMECA, HAZOP studies

System Design Criteria

System design basis

Failure rate data

Chemical and physical processes involved in the plant/ system.

Specific information on the whole process and every stream (e.g., chemistry, thermodynamics, hydraulics)

Hazardous properties of materials (MSDS)

Plant and site layout drawings

Process conditions (PFDs)

System hardware (P&IDs)

Equipment specification

Operation of the plant (operating, maintenance, emergency, start-up, and shut-down procedures)

Human factors [e.g., operations-maintenance, operator-equipment, and instrumentation (man-machine) interfaces]

Environmental factors

1.4.2 수행 절차

Step 1 정상사상(Top Event) 설정

1) 재해의 위험도를 고려하여 해석할 재해를 결정한다.
2) 재해발생 확률의 목표값을 정한다.

Step 2 대상 플랜트, 프로세스의 특성을 파악

3) 해석하려는 시스템의 공정과 작업내용을 파악한다.
4) 재해과 관련있는 설비 배치도, 재료 배치도, 운전지침서 등을 준비하고 이를 숙지한다.
5) 예상되는 재해에 대하여 과거의 재해사례나 재해통계 등을 활용하여 가급적 폭넓게 조사한다.
6) 재해와 관련있는 작업자 실수(Human Error)에 대하여 그 원인과 영향을 상세히 조사한다.

Step 3 FT 작성

7) 정상사상에 대한 1차 원인을 분석한다.
8) 정상사상과 1차 원인과의 관계를 논리 게이트(Gate)로 연결한다.
9) 1차 원인에 대한 2차 원인(결함사상)을 분석한다.
10) 1차, 2차 원인데 대한 관계를 논리 게이트로 연결한다.
11) 9), 10) 항을 더 이상 분할할 수 없는 기본사상(Basic Event) 까지 반복 분석한다.

Step 4 FT 구조해석

12) 작성된 FT를 수학적처리(Boolean Algebra)에 의해 간소화 한다.
13) 최소 컷세트(Minimal Cut Sets), 최소 패스세트(Minimal Path Sets)를 구한다.
14) 정상사상에 영향을 미치는 중요한 중간 및 기본 사상을 파악한다.

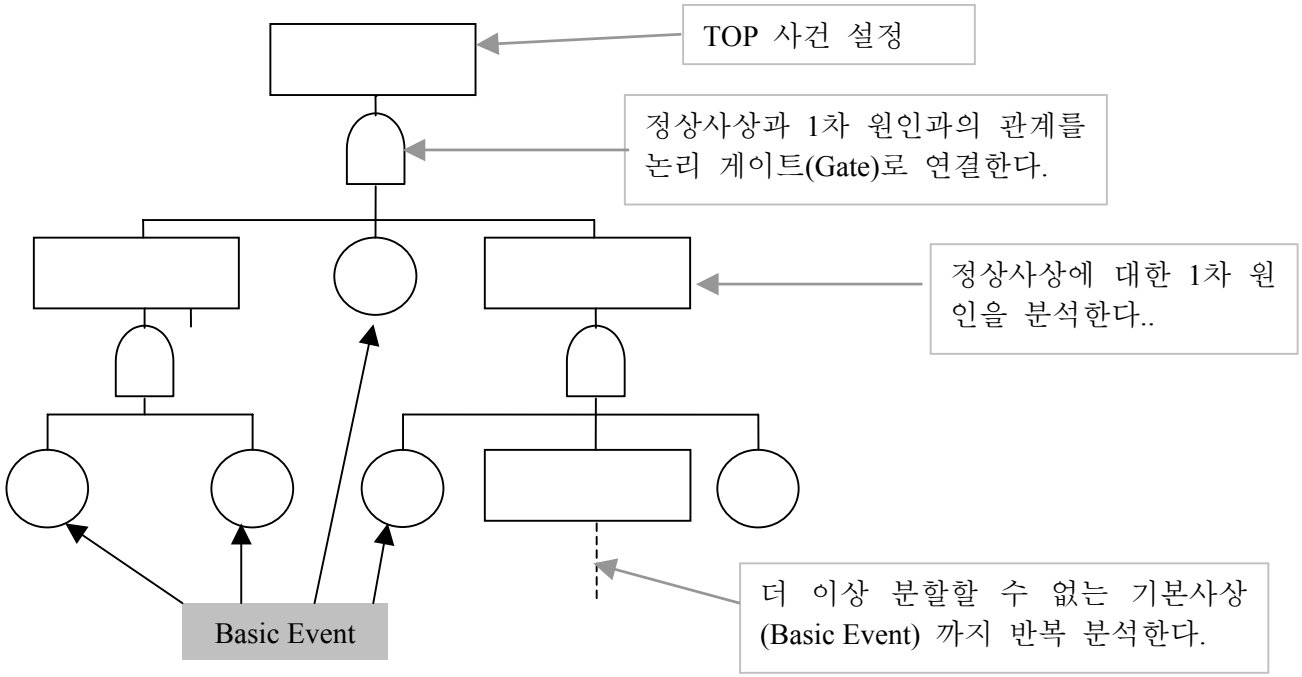
Step 5 FT 정량화

15) 기본사상의 발생빈도나, 고장율, 에러 데이터 등을 정리하여 중간사상 및 정상사상의 발생확률을 계산한다.
16) 재해발생 확률 계산 결과는 과거의 재해 또는 유사한 재해의 발생률과 비교하고 현격한 차이가 날 경우는 작성된 FT에 대하여 재검토를 한다.

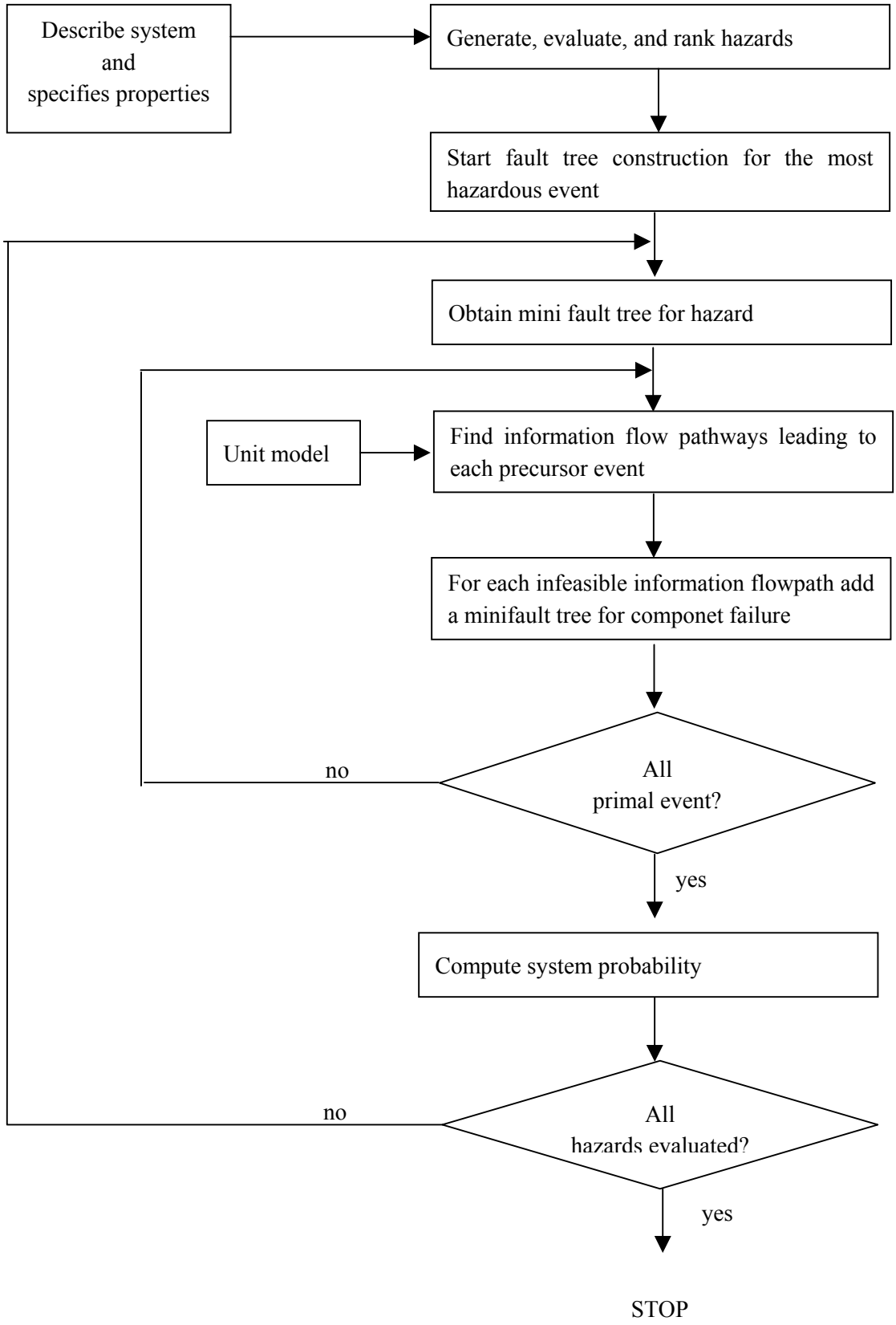
Step 6 해석 결과의 평가

17) 재해 발생 확률이 허용할 수 있는 위험수준을 초과할 경우 이것을 감소시키기 위한 대책을 수립한다.

1.4.3 FT 작성 단계

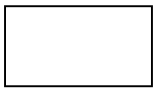
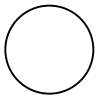
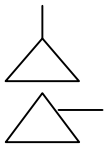
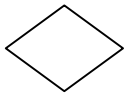

TOP 사건 설정
정상사상과 1차 원인과의 관계를 논리 게이트(Gate)로 연결한다.
정상사상에 대한 1차 원인을 분석한다..
Basic Event
더 이상 분할할 수 없는 기본사상 (Basic Event) 까지 반복 분석한다.

1.4.4 FT 작성 전략 알고리듬

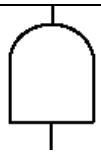
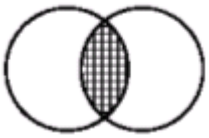
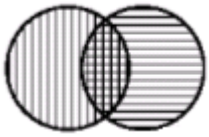


1.5 FT기호

1.5.1 사상기호

기 호		내 용
	사상 Event	개개의 사상 보통 결함사상을 표시 논리기호의 입력 또는 출력
	기본사상 Basic Event	더 이상 전개하지 않는 기본적 사상 논리기호의 입력 논리기호의 출력은 되지 않음
	전입(In) 전출(Out)	동일한 FT속에서 내용이 같은 타부분과의 사이에 전이를 나타내는 기호로서 삼각형의 상부에 선이 나오는 경우는 타부분에서의 전입을 의미하고 측면에 선이 나오는 경우는 타부분으로의 전출을 나타낸다.
	부전개 사상 (undevelopped event)	정보부족에 의해 분석되지 않거나 또는 분석의 필요가 없는 생략 현상을 나타내는 기호이다.

1.5.2 게이트 기호

기 호		내 용	
	AND Gate		하위의 사건을 모두 만족하는 경우에 사용하는 논리 게이트
	OR Gate		하위의 사건중 하나라도 만족하면 사용하는 논리 게이트

1.6 최소 컷셋과 최소 패스셋(Minimal Cut Sets and Minimal Path Sets)

1.6.1 정의

구성된 FT에서 정상사상이나 중간사상의 발생 확률을 계산하여 이것을 예측하는 것도 중요하지만 정상사상 발생에 영향을 미치는 요소를 파악하는 것도 확률계산 못지 않게 중요하다.

이와 같이 정상사상의 위험성을 효과적이고 경제적으로 감소시키기 위하여 사용되는 방법이 최소 컷셋(Minimal Cut Sets)과 최소 패스셋(Minimal Path Sets)이다.

최소 컷셋과 최소 패스셋은 개개의 기본사상 발생확률과 무관하며 AND와 OR로 구성되는 논리조합의 영향만을 받기 때문에 현실적으로 사업장에 매우 유용하고 즉각적인 FTA가 가능할 수 있는 것이다.

즉, FTA를 이용하여 재해발생 확률을 계산하자면 각각의 기본사상 발생 확률 확보가 전제되어야 하고, 또한 고장율의 신뢰도에 따라 결과의 차이는 엄청나게 클 수 있지만 최소 켓셋과 패스셋은 논리조합의 지배를 받기 때문에 **분석의 오차를 최소화할 수 있는 장점**이 있다.

최소 컷셋이란 여기에 포함되어 있는 모든 기본사상이 일어났을 때 Top사상을 발생시키는 기본사상의 최소 집합이라 정의할 수 있으며 그 기본 사상을 집중 관리함으로써 Top사상의 재해발생확률을 효과적이고 경제적으로 감소시킬 수 있는 것이다.

한편 최소 패스셋이란 여기에 포함되어 있는 기본 사상이 일어나지 않으면 정상사상이 발생하지 않는 기본사상의 집합이라고 정의할 수 있다.

1.7 확률의 평가

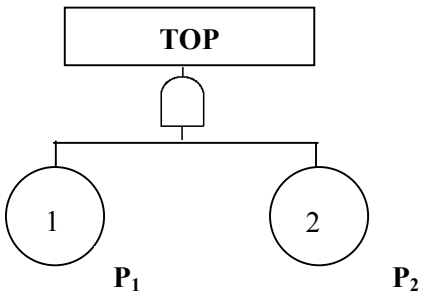
FT를 수식으로 표현하거나 간소화하기 위하여 부울대수(Boolean Algebra)를 사용하는데 이 방법은 논리계산의 한 수단으로서 어느 집합을 구성하는 부분집합들의 논리곱과 논리합을 사용하여 표현하고, 이들의 확률을 계산식을 사용함으로서 FT의 정상사상이나 중간사상, 즉 구하고자 하는 재해발생확률을 계산하는 방법을 말한다.

이때 주의를 요하는 것은 FT내의 2개소 이상에 동일 기본사상이 표함되는 경우의 확률계산은 부울대수에 의한 정리를 행한 후에 실시하지 않으면 전혀 다른 결과가 나올 수 있다는 점이다.

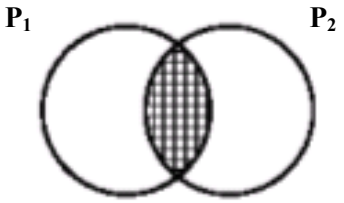
한편 FT가 수많은 기본사상으로 구성된 경우가 많은데 이때는 그것을 몇 개의 부분 FT로 분해하여 각 부분 FT를 해석한 후 전체의 FT를 해석하는 것이 효율적이다.

이와 같은 방법으로 구성된 FT는 AND와 OR게이트로 이루어지며 이들의 해석적 방법에 의한 사상발생 확률을 다음과 같이 표시할 수 있고 기본사상이 서로 통계적으로 독립되어 있다고 가정한 접근 방법이다.

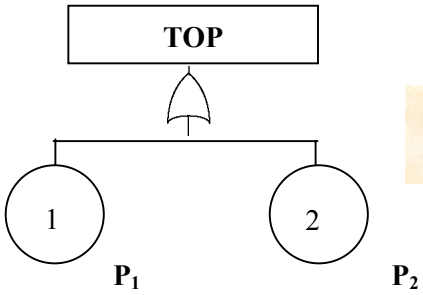
1) AND 게이트



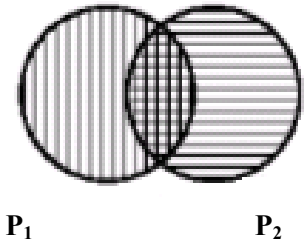
$$P_T = P_1 \times P_2$$



2) OR 게이트



$$P_T = P_1 + P_2 - (P_1 \times P_2)$$



1.8 FTA 활용 및 기대효과

FTA를 이용하여 시각적, 정략적으로 사고원인을 분석하여 재해발생확률이 높은 인적, 물적 환경상의 위험 및 위험사항에 대한 안전대책을 강구하므로서 재해발생확률의 지속적인 감소를 통한 재해예방활동을 체계적이고 과학적으로 수행할 수 있다.

1.8.1 장 점

1) 사고원인 규명의 간편화

사고의 세부적인 원인목록을 작성하여 전문지식이 부족한 사람도 목록만을 가지고 해당사고의 구조를 파악할 수 있다.

2) 사고원인 분석의 일반화

재해발생의 모든 원인들의 연쇄를 한눈에 알기쉽게 Tree상으로 표현할 수 있다.

3) 사고원인 분석의 정량화

FTA에 의한 재해발생 원인의 정량적 해석과 예측, 컴퓨터 처리 및 통계적인 처리가 가능하다.

4) 노력, 시간의 절감

FTA의 전산화를 통하여 최소 컷셋 및 최소 패스셋과 발생확률이 높은 기본사상을 파악하므로서 사고발생에의 기여도가 높은 중요원인을 분석 파악하여 사고예방을 위한 노력과 시간을 절감할 수 있다.

5) 시스템의 결함 진단

복잡한 시스템내의 결함을 최소시간과 최소비용으로 효과적인 교정을 통하여 재해발생 초기에 필요한 조치를 취할 수 있어 재해를 예방할 수 있고 또한 재해가 발생한 경우에는 이를 극소화 할 수 있어 사업체의 높은 관심속에서 폭넓게 이용되고 있다.

6) 안전점검 Check List 작성

FTA에 의한 재해원인 분석을 토대로 최소 컷셋과 재해발생확률이 높은 기본사상을 파악하여 안전점검상 중점을 두어야 할 부분 등을 체계적으로 정리한 안전점검 Check List를 만들 수 있다.

1.8.2 단 점

1) 숙련된 전문가 필요

FTA를 수행하기 위하여는 이 분야에 전문지식을 가진 숙련자가 필요하다. 필요한 전문분야는 통계, 확률 및 컴퓨터 조작은 물론 공정 전반에 걸친 지식과 경험이 풍부하여야 한다.

2) 시간 및 경비의 소요

분석대상 시스템이나 공정의 크기에 따라 소요시간과 경비는 차이가 있을 수 있으나 일반적으로 정성 평가에 비하여 막대한 시간과 경비가 소요된다. 따라서 처음부터 시스템 전체에 대하여 FTA를 시도하지 말고 먼저 정성적 평가를 거친 후 위험도가 높은 시설이나 공정등을 대상으로 수행함이 바람직하다.

3) 고장율 자료확보

성공적인 FTA를 위하여 설비, 부품의 정확한 고장율 확보가 전제되어야 한다. 동일기기, 부품이라 하더라도 사업장, 취급물질, 운전조건 및 작업자의 숙련도에 따라 고장율은 상이하므로 가능한 해당공정 및 시스템에서 발생한 정비자료를 기초로 통계처리를 하여야 높은 신뢰도를 유지할 수 있다.

4) 단일사고의 해석

FTA는 분석 대상 작업이나 공정에서 발생가능한 최악의 사고 시나리오를 가정하여 그 발생 확률과 중요원인을 규명하는 방법으로서 예상치 못한 사고 또는 사소한 위험성은 간과하기 쉽다.

5) 논리게이트 선택의 신중

분석자의 의식중에는 항상 사고확률의 감소라는 개념이 잠재되어 있다고 볼 수 있다. 따라서 특히 AND게이트 선택시에는 논리적으로 타당한가를 신중히 검토하여야 정확한 FTA 결과를 도출할 수 있다.

1.9 FTA 관련 술어 해설

- Risk

A measure of potential economic loss or human injury occurring and the magnitude of the loss or injury if it occurs.

- Risk Assessment

The qualitative or quantitative consideration of accident consequences and probabilities.

- Event

An occurrence involving equipment performance or human action, or an occurrence external to the system that causes system upset.

An unwanted deviation from the normal or expected state of a system component.

- Likelihood

A measure of the expected probability or frequency of occurrence of an event. This may be expressed as a frequency (e.g., events/ years), a probability of occurrence during some time interval, or a conditional probability. (e.g., probability of occurrence given that a precursor event has occurred)

- Rate

The number of events which occur divided by the total operating time. [Time]

- Duration

The length of time for which the event state exists

- Frequency

The average number of time/year that the event (failure, demand, operator action, etc.) occurs. [Time]

A number of occurrences per unit of time.

- Probability

A measure of the uncertainty of the outcome of an event. [Dimensionless]

- Demand

A plant condition which require a protective system or devise to take appropriate action in order to prevent a hazard.

- Fractional dead time

The average probability of the system being in a failed state. [Dimensionless]

The mean fraction of time in which a component or system is unable to operate on demand.

$$FDT = 1/2 \times \Theta \times T \quad \text{if } \Theta \times T \ll 1 \text{ [Times/yr] [yr]}$$

- Hazard rate

The Frequency with which hazards occur.

$$\text{Hazard rate} = \text{Demand rate} \times FDT$$
$$= D \times (1/2) \times \Theta \times T \quad \text{if } \Theta \times T \ll 1 \text{ [Times/yr] [yr]}$$

- (Demand) Logic Diagram

A representation of the sequence of events leading to or from a specified level.

- Top event

The selected outcome whose possible causes are analyzed in a fault tree.

The unwanted event or incident at the "top" of the fault tree that is traced downward to more basic failure using logic gates to determine its causes and likelihood.

- Intermediate event

An event that propagates or mitigates an initiating (basic) event during the accident sequence (e.g., improper operator action, failure to stop an ammonia leak, but an emergency plan mitigates the consequences)

- Basic (Primary) event

A fault tree that is sufficiently basic that no further development is judged necessary (e.g., equipment item failure, human failure, external event)

- Undeveloped event

A base event that is not developed because information is unavailable or historical data are adequate.

- Logic gate

A logical relationship between input (lower) events and a single output (higher) event. These logical relationships are normally represented as AND or OR gate. AND gate combine input events, all of which must exist simultaneously for the output to occur. OR gate also combine input events, but any one is sufficient to cause the output. Other gate types, which are variants of these and are occasionally used, include inhibit gate, priority AND, exclusive OR, and majority voting gate.

- Boolean algebra

That branch of mathematics describing the behavior of linear functions of variables that are binary in nature; on or off, open or closed, true or false. All coherent fault tree can be converted into an equivalent set of Boolean equations.

- Minimal cut set

The smallest combination of component and human failure that, if they all occur, will cause the top event to occur. The failure all correspond to basic or undeveloped events. A top event can have many minimal cut sets, and each minimal cut set may have a different number of basic or undeveloped events. Each event in the minimal cut set is necessary for the top event to occur, and all events in the minimal cut set are sufficient for the top event to occur.

P(success) = number of success / number of possible outcomes

P(failure) = number of failure / number of possible outcomes

s = number of ways success can occur

f = number of ways failure can occur

$P(\text{success}) = p = s / (s + f)$

$P(\text{failure}) = q = f / (s + f)$

$p + q = 1$

1.10 Failure Rates

1.10.1 Failure Rate Data for Various Selected Process Components

Instrument	Fault/ year
Controller	0.29
Control valve	0.60
Flow measurement (fluids)	1.14
Flow measurement (solids)	3.75
Flow switch	1.12
Gas-liquid chromatograph	30.6
Hand valve	0.13
Indicator lamp	0.044
Level measurement (liquids)	1.70
Level measurement (solids)	6.86
Oxygen analyzer	5.65
pH meter	5.88
Analyzer	0.25
Pressure measurement	1.41
Pressure relief valve	0.022
Pressure switch	0.14
Solenoid valve	0.42
Stepper motor	0.044
Strip chart recorder	0.22
Thermocouple temperature measurement	0.52
Thermometer temperature measurement	0.027
Valve positioner	0.44

Selected from Frank P. Lees, Loss Prevention in the Process Industries (London: Butterworths, 1986) p.343

1.10.2 Human failure rates data

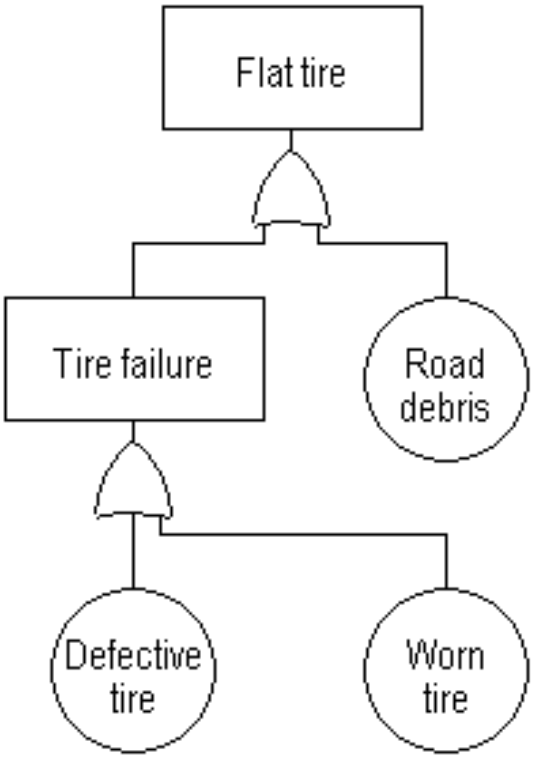
Activity	Error Rate
*Error of omission/ item embedded in procedure	0.003
*Simple arithmetic error wih self-checking	0.03
*Inspector error of operator oversight	0.1
*General rate/ high stress/ dangerous activity	0.2-0.3
*Checkoff provision improperly used	0.1-0.09 (0.5 avg.)
**Error of omission/10-item checkoff list	0.0001-0.0005 (0.0001 avg.)
**Carry out plant policy/ no check on operator	0.005-0.05 (0.01 avg.)
**Select wrong control/group of identical, labeled, controls	0.001-0.01 (0.003 avg.)

* WASH-1400 (NUREG-75/014); "Reactor Safety Study – An assessment of Accident Risks in U.S. Commercial Nuclear Power Plants." 1975

**NUREG/CR-1278; "Handbook of Human Relliability Analysis with Emphasis on Nuclear Power Plant Applications.' 1980

1.11 FTA 실행 예

1.11.1 Flat tire



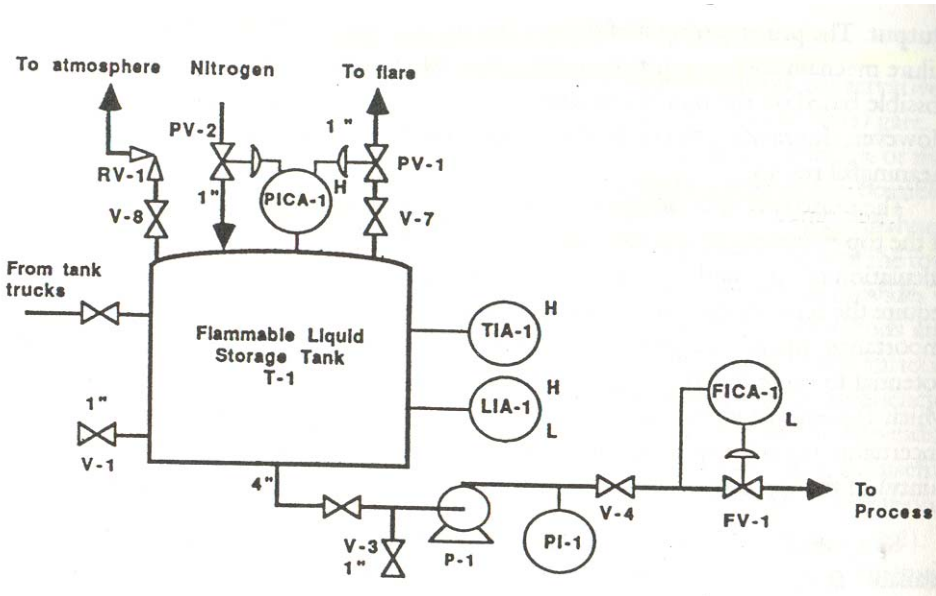
1.11.2 Example 1

Step 1. System Description. The P&ID for the storage tank system is given. The storage tank (T-1) is designed to hold a flammable liquid under slight nitrogen positive pressure. A control system (PICA-1) controls pressure. In addition, the tank is fitted with a relief valve to cope with emergencies. Liquid is fed to the tank from tank trucks. A pump (P-1) supplies the flammable liquid to the process.

Step 2. Hazard Identification. HAZOP was used to identify the most serious hazard as a major flammable release from the tank. This incident is the top event that will be developed in the fault tree.

Step 3. Construction of the Fault Tree. Based on the knowledge of the system and initiating events in the HAZOP study, the tree is constructed manually. Every event is labeled sequentially with a B for basic or undeveloped event, M for intermediate event, and T for the top event. The procedure starts at the top event, major flammable release, and determines the possible events that could lead to this incident as

M1: Spill during truck unloading
M2: Tank rupture due to external event
B1: Tank drain breaks
M3: Tank rupture due to implosion
M4: Tank rupture due to overpressure



Events M1, M2, M3, and M4 require further development. However, adequate historical/ reliability data exist for Event B1 to allow it to be treated as a basic event. The analysis proceeds downward, on level at a time, until all failure mechanisms have been investigated to the appropriate depth. The basic events and undeveloped events are symbolized by circles and diamonds, respectively. Further development of the undeveloped events is not thought mecessary or possible.

Step 4. Qualitative Examination of Structure. The qualitative ranking is best done using minimal cut set analysis for this problem. However, inspection alone shows the five major mechanisms leading to major flammable release. For example, the single events B1, B3, B4, B5, and B6 all lead to the top event. In this example, qualitative ranking is of limited benefit as a frequency value is wanted for CPQRA.

In this step, the analyst should review the minimal cut sets to ensure that they represent real, possible, accidents. A minimal cut set that will not cause the top event is an indication of an error in the construction of the fault tree or in the determination of the minimal cut sets.

Setp 5. Quantitative Evaluation of Fault Tree. For this example, the method of gate-by-gate analysis is employed to quantify the fault tree. The tree must be carefully scanned for repeated events, as these can lead to numerical error. There are no repeated events. The analyst must enter a numerical value for frequency (per year) or probability (dimemsionless) into every base event.

The calculation starts at the bottom of the tree and proceeds upward to the top event. A calculation is presented for the left most branch of the tree to event M1, spill during truck unloading. For clarity, only one significant figure is used in this example.

The lowest gate is M9, tank overfill and release via RV-1. The two inputs to this AND gate are probabilities.

$$P(M9) = P(B15) \times P(B16) = (1 \times 10^{-2}) \times (1 \times 10^{-2}) = 1 \times 10^{-4}$$

At the same level as M9 is Gate M10, tank rupture due to reaction. There are four inputs to this AND gate

$$P(M10) = P(B17) \times P(B18) \times P(B19) \times P(B20)$$
$$= (1 \times 10^{-3}) \times (1 \times 10^{-2}) \times (1 \times 10^{-1}) \times (1 \times 10^{-1}) = 1 \times 10^{-7}$$

Gate M9 and M10 are inputs to Gate M5, major tank spill. There are two probabilities entering the OR gate;

$$P(M5) = 1 - [1 - P(M9)][1 - P(M10)]$$
$$P(M5) \approx P(M9) + P(M10) \approx (1 \times 10^{-4}) + (1 \times 10^{-7}) = 1 \times 10^{-4}$$

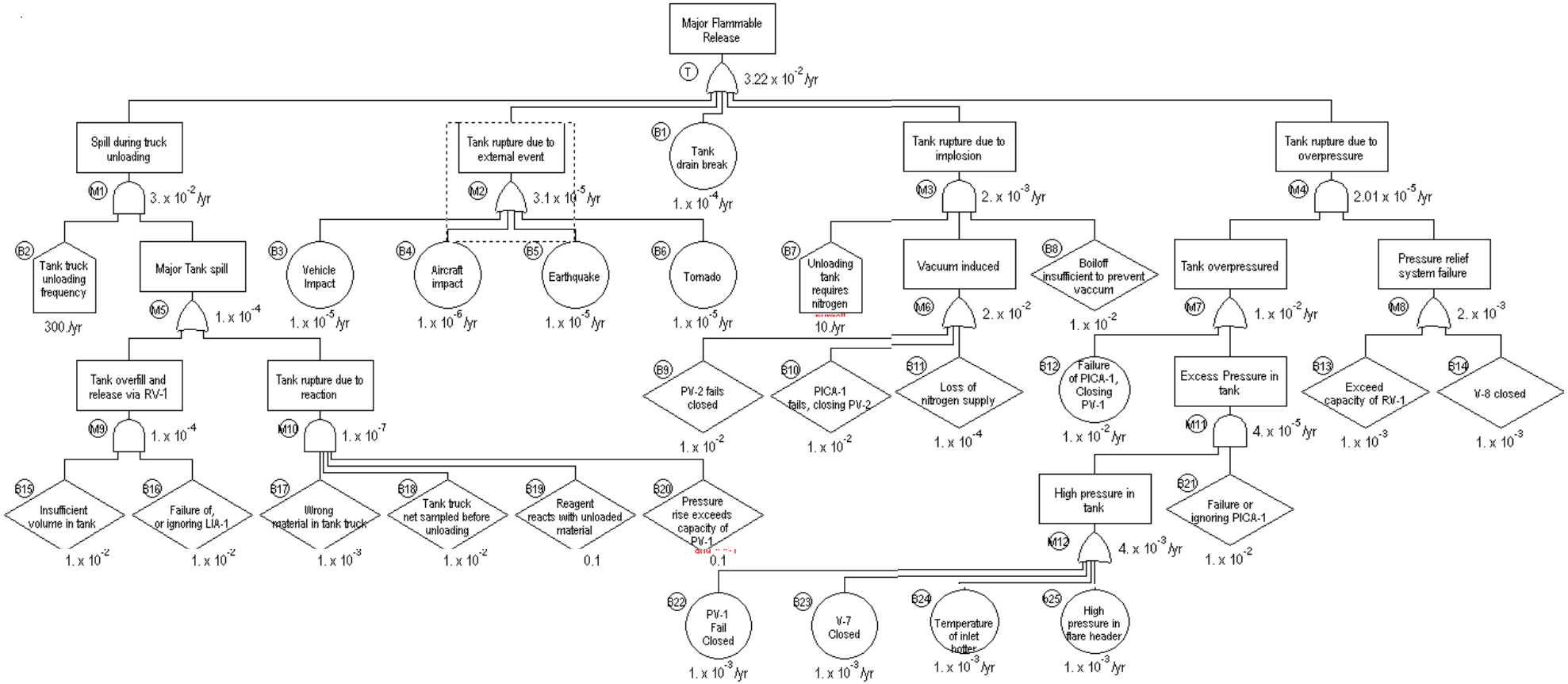
Gate M1 is an intermediae event arm and is an AND gate with two inputs, a frequency and a probability

$$F(M1) = F(B2) \times P(M5) = (300/yr) \times (1 \times 10^{-4}) = 3 \times 10^{-2}/yr$$

In a similar manner, all other frequencies and probabilities may be calculated, up to the top event. The top event frequency (T), major flammerble release, is 3×10^{-2}/yr on a release of every 30 years.
The frequencies of the five major intermediate events leading to this are

M1: Spill during truck unloading	3×10^{-2}/yr
M2: Tank rupture due to external event	3×10^{-5}/yr
B1: Tank drain break	1×10^{-4}/yr
M3: Tank rupture due to implosion	2×10^{-3}/yr
M4: Tank rupture due to overpressure	2×10^{-5}/yr

From the quantitative evaluation, the failures due to M1 and M3 contribute most to the top event; frequency and remedial measures would be most productively employed in these areas.


Major Flammable Release
T
3.22 x 10^-2 /yr
Spill during truck unloading
M1
3. x 10^-2 /yr
Tank rupture due to external event
M2
3.1 x 10^-5 /yr
B1
Tank drain break
1. x 10^-4 /yr
Tank rupture due to implosion
M3
2. x 10^-3 /yr
Tank rupture due to overpressure
M4
2.01 x 10^-5 /yr
B2
Tank truck unloading frequency
300 /yr
Major Tank spill
M5
1. x 10^-4
B3
Vehicle Impact
1. x 10^-5 /yr
B4
Aircraft impact
1. x 10^-6 /yr
B5
Earthquake
1. x 10^-5 /yr
B6
Tornado
1. x 10^-5 /yr
B7
Unloading tank requires nitrogen
10 /yr
Vacuum induced
M6
2. x 10^-2
B8
Boiloff insufficient to prevent vaccum
1. x 10^-2
Tank overpressured
M7
1. x 10^-2 /yr
Pressure relief system failure
M8
2. x 10^-3
Tank overfill and release via RV-1
M9
1. x 10^-4
Tank rupture due to reaction
M10
1. x 10^-7
B9
PV-2 fails closed
1. x 10^-2
B10
PICA-1 fails, closing PV-2
1. x 10^-2
B11
Loss of nitrogen supply
1. x 10^-4
B12
Failure of PICA-1, Closing PV-1
1. x 10^-2 /yr
Excess Pressure in tank
M11
4. x 10^-5 /yr
B13
Exceed capacity of RV-1
1. x 10^-3
B14
V-8 closed
1. x 10^-3
B15
Insufficient volume in tank
1. x 10^-2
B16
Failure of, or ignoring LIA-1
1. x 10^-2
B17
Wrong material in tank truck
1. x 10^-3
B18
Tank truck net sampled before unloading
1. x 10^-2
B19
Reagent reacts with unloaded material
0.1
B20
Pressure rise exceeds capacity of PV-1
0.1
High pressure in tank
M12
4. x 10^-3 /yr
B21
Failure or ignoring PICA-1
1. x 10^-2
B22
PV-1 Fail Closed
1. x 10^-3 /yr
B23
V-7 Closed
1. x 10^-3 /yr
B24
Temperature of inlet hotter
1. x 10^-3 /yr
B25
High pressure in flare header
1. x 10^-3 /yr

1.11.2 Example 2

Given a particular LPG tank BLEVE frequency of 1 x 10^{-6} per year and a nearby public area usage frequency of 10 times per year (8hr exposure each), an AND gate frequency combination of BLEVE and people affected should be converted to frequency of BLEVE and conditional probability of people present. This probability is

(10 times/yr x 8hr)/(365 days/yr x 24hr/day) = 0.009

The AND gate result = 1 x 10^{-6} per year x 0.009 = 9 x 10-9 per year frequency of affecting the public from the BLEVE.