

Digraph를 이용한 Fault Tree 자동합성

이근원 · 정원석 · 문일*

한국산업안전공단 산업안전보건연구원 · 연세대학교 화학공학과

서론

화학공정에서 발생하는 사고의 주요 원인으로는 조업자의 실수, 장치고장, 안전장치의 미비, 운전조건의 이상을 들 수 있다. 화학공정의 위험 분석은 HAZOP, FTA, ETA, 및 CA 등이 산업계에서 가장 유용하고 폭넓게 사용되고 있는 분석 방법이다. 이들 위험분석 기법 중에서 FTA(Fault Tree Analysis)는 사고의 세부적인 원인목록을 작성하여 해당사고의 구조를 파악할 수 있으며 복잡한 시스템내의 결함을 최소시간과 최소비용으로 효과적으로 예방할 수 있게 하는 정량적 위험성 평가 방법이다. 일반적으로 이 방법들은 전문가 집단에 의해 수행되기 때문에 전문가 집단의 능력과 투여 되는 시간에 많이 비례하여 왔던 것이 사실이다. 이러한 이유로 인하여 위험분석방법의 자동화가 절실히 대두되고 있는 실정이다.

과거 20여년에 걸쳐 FTA자동화에 대한 연구가 많이 진행되어 오면서 여러 학자들에 의해 효율적인 도구들이 개발되어 FT 구성에 사용되어져 왔는데, Transfer function (Fussell, 1973), Decision Table (Salem et al., 1977), Digraph (Lapp and Powers, 1977), Reliability Graph(Camarda et al, 1978), Mini Fault Tree(Kelly and Lees, 1986) 등이 그것들이다. 그러나 아직까지 확률 계산 부분이나 minimal cutset 산출부분을 제외하고는 자동화가 진행된 부분이 거의 없는 것이 사실이다. FT 생성에 있어 발생할 수 있는 시간적 소요와 인적 오류를 해결하기 위해서는 객관적인 규칙이 존재하는 FT 자동합성 시스템이 절실하다.

본 연구에서는 FT 자동합성시스템을 위한 공정의 효율적인 표현 방법으로는 Digraph(Directed Graph)를 이용하였다. PFD(Process Flow Diagram)나 P&ID(Piping & Instrumentation Diagram)로부터 사용자가 작성한 Digraph(Directed Graph)를 적합한 형태의 자료로 입력, 자동으로 FT(Fault Tree)가 생성되도록 Digraph-FT 전환 알고리즘을 개발하였고, 사고의 원인을 기존의 원인과 함께 공정변수의 이상에서 찾아 주는 FT 자동합성 시스템을 개발하여 대상공정에 적용하여 보았다.

Digraph-FT 전환 알고리즘

본 연구에서 개발한 Digraph-FT 전환 알고리즘은 Fig 1과 같다. 분석하고자 하는 공정에 대하여 Digraph를 구성하고, 선정된 Top event가 놓여 있는 상황에 따라 각각의 FT 생성 규칙을 적용하였다. 선택한 사고, 즉 Digraph 상에서의 노드에 대하여 FT 생성규칙을 적용한 후에 다시 반복적으로 각각의 노드에 대해 규칙을 적용하면서 기초 사상(Basic event)이 나타날 때까지 알고리즘을 반복적으로 수행하게 하였다.

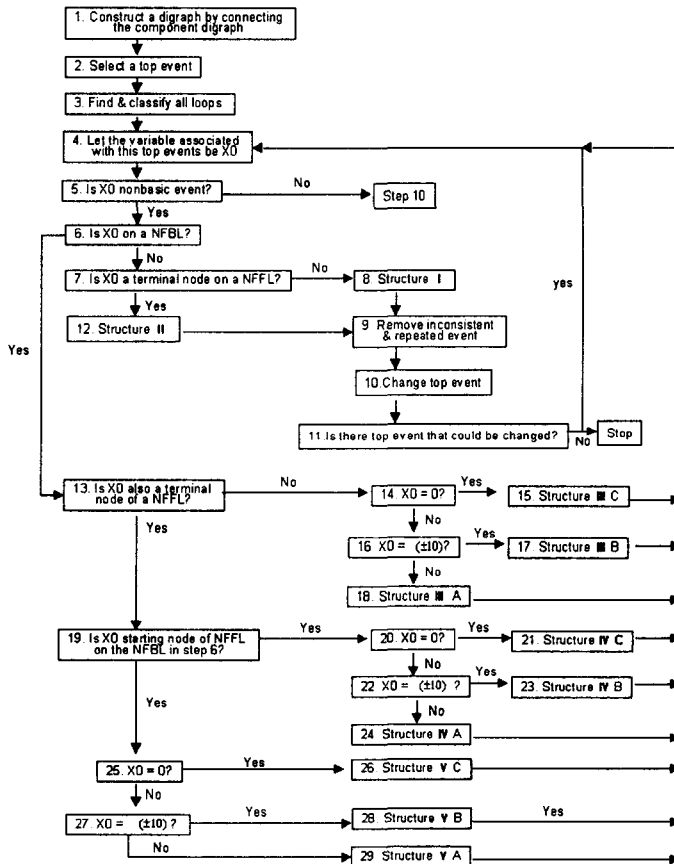


Fig. 1 Digraph-FT conversion algorithm

FT 자동합성시스템은 분석자가 선정된 Top event와 관련 있는 루프를 찾아 주고, 각각의 경우에 대하여 FT 생성규칙을 적용하여 FT를 자동 합성하게 된다. FT 생성규칙

은 노드가 놓여 있는 상황에 따라 다음과 같이 구분하였다.

(1) Structure I

- 루프에 있지 않는 경우
- PFFL, PFBL 에 있는 경우
- NFFL에 있으면서 종말노드가 아닌 경우

(2) Structure II

- NFFL의 종말노드인 경우

(3) Structure III

- NFBL에 있는 경우

(4) Structure IV

- NFFL의 종말노드가 NFBL에 있으면서, NFFL의 시작노드는 NFBL에 있지 않을 경우

FFL(Feedforward loop)은 시작 노드와 종말노드가 서로 다른 루프이고, FBL(Feedback Loop)은 시작노드와 종말노드가 동일한 루프로서 각각의 gain의 곱이 양이나 음이냐에 각각 PFFL, NFFL, PFBL, NFBL로 분류하였다.

대상공정에의 적용

본 연구에서 개발한 알고리즘을 Fig. 2의 대상공정에 적용해 보았다. 선택한 공정은 hot nitric acid가 nitration reactor에서 benzene과 혼합되기 전에 냉각시켜 주는 공정이다. 흐름 4의 배출물 온도는 온도센서와 역반응 온도 제어를 통한 FBL에 놓여 있어서 배출물의 과도한 온도가 감지 될 때는 밸브 1을 닫게 되어있고, pump shutdown이 발생하였을 때는 밸브2가 닫게 되어있다.

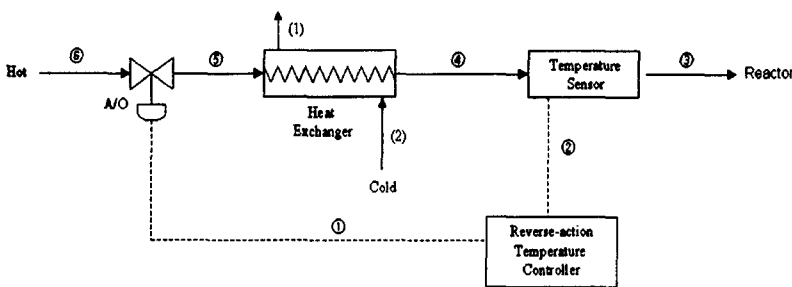


Fig. 2 Nitric acid cooler with temperature feedback and pump shutdown feedforward loops

Fig. 2의 공정도로부터 Digraph를 구성해 보면 Fig. 3과 같다. 공정도의 각 흐름별로 온도, 압력, 유량을 노드로, 장치의 고장, 조업자의 실수 등을 결함으로 표현하였다. Digraph 상에서 각각의 노드, 즉 공정도상의 공정 변수간의 관계는 gain으로 표현된다. Gain은 유입흐름의 공정변수의 변화량당 출력흐름의 변화량을 의미는 것으로서 (0), (1), (10)의 값을 갖는다. 공정변수의 변화량 역시 (0), (1), (10)의 값을 갖는다. 각각의 값의 결정은 대상공정의 장치에 따라 제시되는 설계값과 운전값을 참고로 사용자가 결정하게 된다. 예를 들어 보면 그림 3의 펌프로부터 열교환기로 들어가는 흐름 8의 유량(M8)이 적당히 증가하면 열교환기로부터 나가는 흐름 3의 온도(T3)가 적당히 감소하게 된다. 따라서 Digraph 상에서 M8 노드와 T3노드는 (-1)의 gain을 가지는 관계로 표현되게 된다.

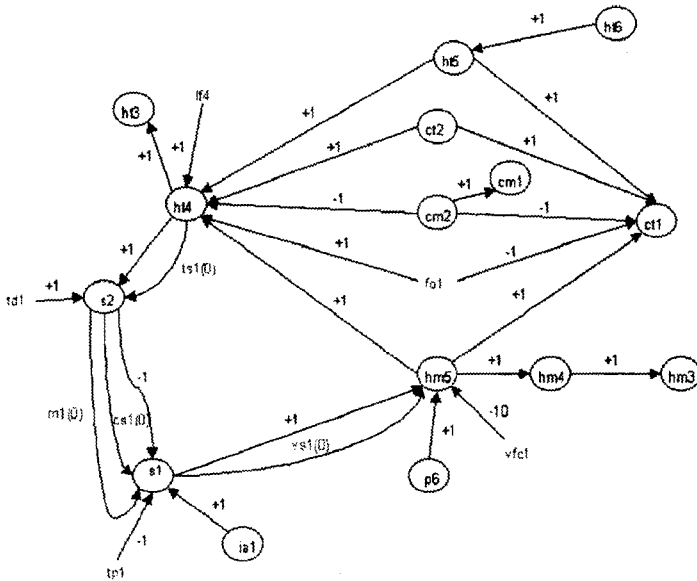


Fig 3. Digraph for heat exchange system

Fig. 3에서 살펴보면 T3는 [T3P6P7M2]의 경로를 가지면서 gain의 곱이 음인 NFBL

에 존재하게 된다. 따라서 T3를 분석하게 될 경우 Structure III가 적용되게 된다. 주어진 공정에서 반응기로 유입되는 흐름의 온도가 증가하는 것, 즉 T4(+1)을 Top event로 선정하여 FT를 구성해 보면 Fig. 4와 같은 결과를 얻을 수 있다. 결과를 분석해 보면 대상공정의 흐름 4의 유출물의 온도가 증가하여 일어 날 수 있는 사고의 원인으로 공정내의 여러 장치의 고장과 공정변수의 변화를 찾아 낼 수 있었다. 예제 공정에서 흐름 5의 Hot stream의 유량이 증가하는 hm5(+1)을 Top event로 선정하여 FT를 구성해 보면 Fig 4와 같은 결과를 얻을 수 있다.

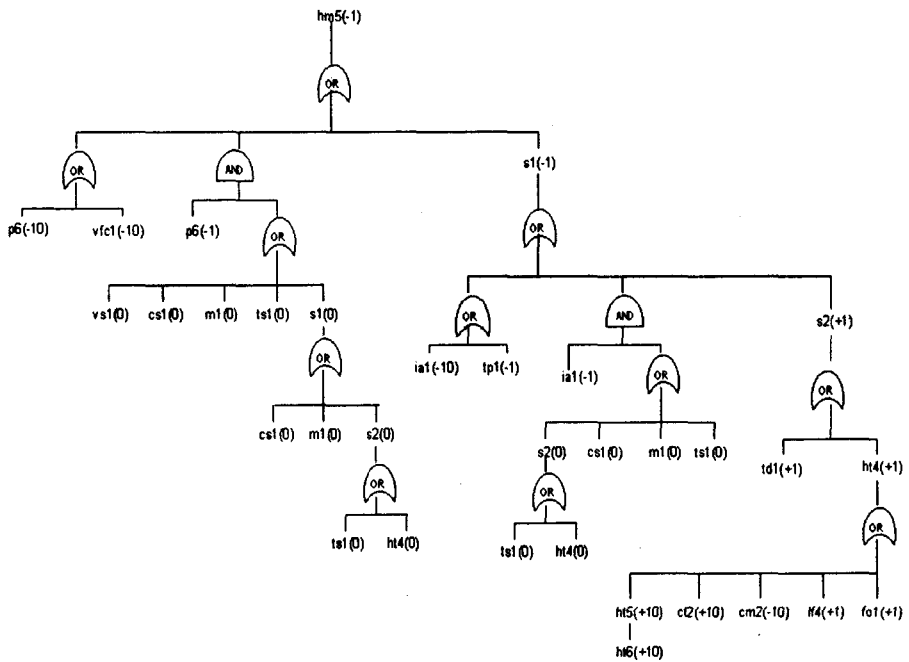


Fig 4. Fault tree for heat exchange system

결론

본 연구에서는 Digraph-FT 전환 알고리즘을 이용하여 효율적인 FT 자동 합성 시스템을 개발하였다. 상황별 FT 합성에 대한 객관적인 규칙을 설정함으로써 사용자의 사전지식에 의존되던 위험성 평가의 단점을 극복할 수 있었다. 또한 기존에 위험성평가 결과로 제시되던 공정안전 개선방안이 조업자의 실수 감소방안, 안전장치의 설치 등에 국한되었던 것에 반해 본 연구에서는 개발한 FT 자동합성시스템은 공정변수에 중점을 두어 위험성 평가를 수행함으로써 공정 운전조건의 변화를 통한 안전성 향상을 이룰 수 있다. 기존의 사용자가 수행하던 FT가 공정에 대한 전문적인 지식과 분석자의 능력에 따라 다른 결과가 나오는 단점을 본 연구에서 개발한 시스템을 이용하면 개선할 수 있을 것으로 기대된다.

참고문헌

1. Allen, D. J., Digraphs and fault Tree, Ind. Eng. Chem. Fundam., Vol. 23, 1984.
2. Andrews, J. D and Brennan, G., "Application of the digraph method of fault tree construction to a complex control configuration", Rel. Eng. and Sys. Saf., Vol. 28, 1990.
3. Dong-Hsiung Kuo, Ding-Shang Hsu, Chuei-Tin Chang, and Dong-Han Chen, Prototype for integrated hazard analysis, Proc. Sys. Engng. Vol. 43, 1997.
4. Kramer M. A. and Palowitch Jr., A rule-based approach to fault diagnosis using the signed directed graph, AIChE J., Vol. 33, 1987.
5. Lapp, S. A and Powers, G. J., "Computer-aided synthesis of fault trees", IEEE Trans. Rel., 1977.
6. Narsingh D., Graph theory with applications to engineering and computer science, Prentice-Hall, Cal, 1974.
7. 이한용, 김진경, 문일, "회분공정의 안전성 평가를 위한 모델 검증 기법의 적용", 화학공학 37권, 6호, 1999.
8. 주종대 등, "화학공정위험성평가Ⅱ(사고빈도 분석)", 한국산업안전공단, 2000.