KIGAS Vol.5, No.2, June, 2001
(Journal of the Korean Institute of Gas)

객체지향 장치 모델링을 이용한 Fault Tree의 자동합성

허 보 경 · †황 규 석
부산대학교 화학공학과
(2001년 1월 4일 접수, 2001년 3월 21일 채택)

Automatic Synthesis of Fault Tree Using Object-oriented Unit Modeling

Bo Kyeng Hou · Kyu Suk Hwang
Dept. of Chem. Eng., Pusan National University, Pusan 609-735, Korea
(Received 4 January 2001 ; Accepted 21 March 2001)

요 약

공정의 위험성 평가를 위한 이상트리 작성은 많은 시간과 인력을 요하는 작업으로 대규모 화학공장에 적용하기가 매우 힘들다. 본 연구에서는 화학공정의 이상트리 합성을 위해 장치에서 발생할 수 있는 공정변수의 이탈 및 장치이상에 대한 원인-결과 관계를 나타내는데 필요한 객체지향 지식기반의 프레임워크를 제안하였다. 이상에 대한 원인을 탐색하기 위하여 장치의 객체지향 모델링과 장치간의 연결관계를 이용하여 이탈을 전파하고 이를 통해 이상트리를 합성하였다. 제안된 방법론을 질산 냉각 공정에 적용하여 그 유효성을 검증하였다.

Abstract - Fault tree construction for hazard assessment requires so much time and labor, so it is very difficult to be applied to the large scale chemical plant. In this study, for the synthesis of fault tree in chemical processes, the object-oriented knowledge framework is proposed to represent the deviations of process variables in the equipment and cause-consequence relationship with equipment faults. The cause of fault is searched by using the object-oriented modeling of equipments and the connectivity among equipments, and then a fault tree is synthesized. we have discussed the performance of the methodology on nitric acid cooling process to evaluate its effectiveness.

Key words : Object-oriented knowledge framework, Fault tree, Cause-consequence relationship

1. 서 론

이상트리(FT)의 작성은 많은 시간과 노력을 필요로 하는 작업으로 복잡하고 규모가 큰 화학공정에 이를 적용하는 것은 대단히 힘들다. 따라서 최근 이러한 문제를 해결하기 위하여 FT의 작성 및 분석과정을 컴퓨터를 이용하여 자동화하려는 연구가 많이 진행되고 있다.

FT합성을 위한 모델링 방법은 크게 장치 중심(componentistic) 또는 기능중심(functional)의 2가지 접근법으로 나눌 수 있다. 장치중심의 모델링 방법은 각각의 장치들에서 발생할 수 있는 이상에 대한 원인-결과 관계 및 그 장치들 사이의 연결관계를 이용하여 합성하는 방법으로써 장치의 국부적인 거동을 상세하게 나타낼 수 있는 장점이 있지만, 대상공정의 전체

†주저자 : kshwang@hyowon.pusan.ac.kr

적인 거동과 제어루프의 문제를 나타내는 데에는 어려움이 있다. 기능중심의 모델링 방법은 대상공정을 제어루프, 트립루프, by-pass line, stand-by line과 같은 기능구조를 중심으로 유향그래프(diagraph)를 작성하여 이상트리를 합성하는 방법으로 대상공정의 전체적인 거동을 보다 더 잘 나타낼 수 있는 장점이 있지만, 대상공정의 변경 시에는 유향그래프의 재작성이 불가피한 단점이 있다[1-3]. 본 연구에서는 화학공장에서 발생할 수 있는 중대한 위험사건을 각각의 장치별로 발생 가능한 최상위사건으로 제시하고, 화학공장의 일반적인 장치에서 발생할 수 있는 공정변수의 이탈 및 장치이상에 대한 원인-결과 관계를 객체지향 지식 기반으로 표현하여 대상공정이 바뀌는 경우에도 해당장치의 룰을 그대로 이용하거나 또는 추가 및 변경하여 FT를 합성할 수 있도록 유연성을 부여한다. 발생할 수 있는 이상에 대한 원인을 탐색하기 위해 장치의 특성 및 장치간의 연결관계를 이용하여 이탈을 전파하고 이를 통하여 FT를 합성한다.

2. FT의 자동합성

2.1. 지식베이스의 구조

화학공정에서 발생 가능한 사건은 장치의 leak 또는 막힘 등의 세부적인 사건과 이러한 사건에 의해 야기되는 유량의 감소, 압력의 증가 등과 같은 공정변수의 이탈사건, 그리고 이러한 두 사건들에 의해 야기되는 장치의 파괴 및 폭발 등의 큰 사건으로 나눌 수 있다. 본 연구에서는 이러한 세 가지 레벨의 사건에 대하여 장치의 파괴 및 폭발 등의 큰 사건은 화학공정의 각각의 장치에서 발생할 수 있는 중대한 사건으로 분류하여 그 원인-결과관계를 최상위사건 지식베이스로 구축하였다. 그리고 나머지 두 가지 사건들은 장치 종류, 운전상태 및 연결관계를 고려하여 그 원인-결과 관계를 장치지식베이스로 구축하였다.

2.1.1. 최상위사건 지식베이스(Top Event knowledge base)

FT를 작성하기 위해서는 먼저 해석하고자하는 최상위 사건을 결정해야 한다. 일반적으로 화학공정에서 발생 가능한 중요한 사건은 폭발, 화재, 누출 등의 사건으로 Pipe 및 반응기에 대한 예를 Fig. 1에 나타내었다. 이와 같은 사건들은 화학공정내의 어떤 한 장치에서 발생하여 결국에는 공장전체의 대형사건으로 확대되어지므로 본 연구에서는 이를 각각의 장치에서 발생 가능한 사건으로 정의하여 IF-THEN rule을 이용하여 지식베이스화 하였다.

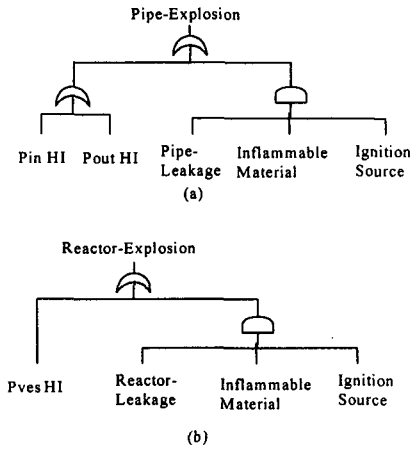

Fig. 1. Sample of top event model
(a) pipe exlosion,
(b) reactor explosion

예를 들어 Reactor에 있어서 압력의 증가와 같은 사건은 반응물질의 유량증가에 의하거나 반응기 내의 온도상승에 의하여 야기된다. 그리고 반응기 내의 온도상승은 반응기로 유입되는 물질의 온도상승 또는 Reactor 외부의 냉각수의 이상에 의하여 야기된다. 이러한 유량, 농도, 온도, 압력, 액위 등의 공정변수의 이탈에 대한 세부적인 원인은 장치 지식베이스에서 다루었다.

2.1.2. 장치 지식베이스

장치 지식베이스(component knowledge base)는 장치의 종류별로 운전상태 및 연결관계에 따라 각각의 장치에서 발생 가능한 사건들에 의하여 야기되는 공정변수의 이탈에 대한 원인-결과관계가 프레임과 룰의 형태로 저장되어 있는 부분이다. 룰은 계층적 장치 트리(hierarchical unit tree)에서 상위의 클래스로부터 하위의 클래스로 상속되므로 최하위 클래스에서 실례에 해당하는 장치는 해당 장치의 특

정한 룰만 추가 및 변경함으로써 효과적인 지식베이스 관리가 가능하다(Fig. 2).

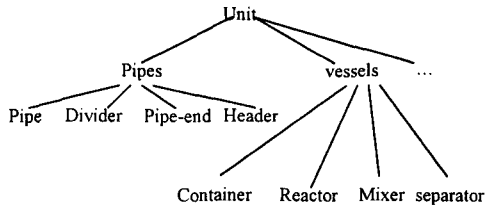

Fig. 2. Hierarchical unit tree

본 연구에서 다루는 장치와 장치고장 및 변수(Variables)와 변수의 이탈(Deviation)을 Table 1과 2와 같이 정의하였다.

Table 1. Component and component failure

Component, etc		Component Fail/Failure State	
Abbrev.	Meaning	Abbrev.	Meaning
CL	Control Loop	PB	Partial Blockage
CNT	Controller	CB	Completely Blockage
CV	Control Valve	LK	Leakage
HV	Hand Valve	HA	High Aperture
SEN	Sensor	LA	Low Aperture
POW	Power supply	NA	No Aperture
SL	Signal Line	LOS	Loss
HEX	Heat Exchanger	STK	Stuck
RXT	Reactor	MAN	Manual
TNK	Tank	F	Fail
RV	Relief Valve		

Table 2. Abbreviation of variables, deviation, subscript and meanings

Variables		Variable Deviation		Variable Subscript	
Abbrev.	Meaning	Abbrev.	Meaning	Abbre.	Meaning
F	Flow	HI	High	1, 2, ...	Port
G	Gradient	LO	Low	IN	Inlet
T	Temperature	NO	None	OUT	Outlet
P	Pressure	REV	Reverse	VES	In Vessel
L	Level				
S	Signal				
SP	Set Point				
X	Composition				

각 장치에서 발생 가능한 사건에 대한 원인-결과 지식베이스를 구축하기 위하여, 어떤 한 공정변수의 이탈에 의하여 야기되는 다른 공정변수들의 이탈은 전파식(Propagation Equation)을 이용함으로써 공정변수간의 상관관계를 유도할 수 있으며, 이와 함께 장치의 고장에 의해 야기되는 변수의 이탈을 동시에 고려하여 이를 IF-THEN 룰로 나타내어 THEN부에 각각의 장치에서 발생할 수 사건을 나타내고 IF부에는 해당사건에 대한 원인사건을 나타내어 후향추론에 의하여 발생한 사건에 대하여 그 원인사건의 탐색이 가능하게끔 하였다(Fig. 3). 예를 들어, Pipe에 대한 전파식은 F2out = f(+G1in, +G2out), G1in = f(+F1in, +F2out), T2out = f(+T1in), X2out = f(+X1in) 등으로 나타낼 수 있다. 상기 전파식의 의미는 우변의 공정변수의 기호가 +의 경우에는 우변의 항이 증가함에 따라 좌변의 항도 증가하는 비례관계를, -의 경우는 우변이 증가함에 따라 좌변의 항이 감소하는 반비례관계를 나타낸다.

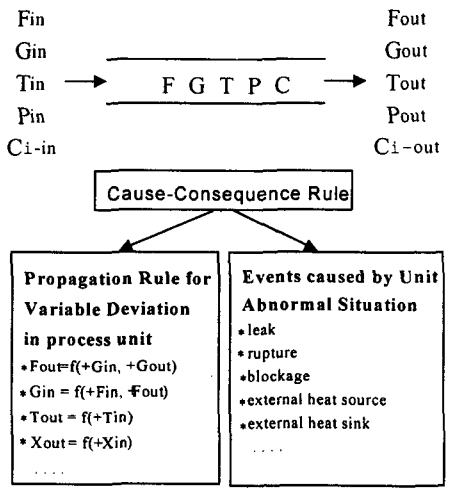

Fig. 3. Scheme of component knowledge base

따라서 전파식으로부터 유도할 수 있는 변수간의 상관관계와 장치의 이상에 의한 공정변수의 이탈을 룰로 나타낼 수 있다. Pipe의 출력 2에서의 유량과 온도의 이탈에 관한 룰을 fault tree형태로 나타내면 Fig. 4와 같다. 여기

서 G는 inlet, F는 outlet에서만 정의를 하여 이를 통해 이탈에 대한 원인을 탐색할 때 양방향 전파가 가능하다.

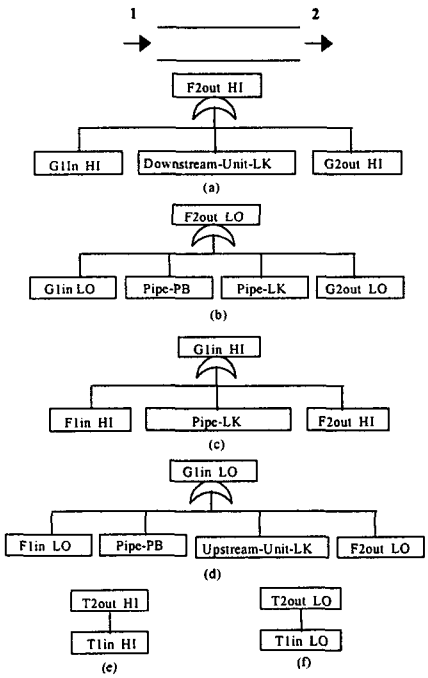

Fig. 4. Pipe model

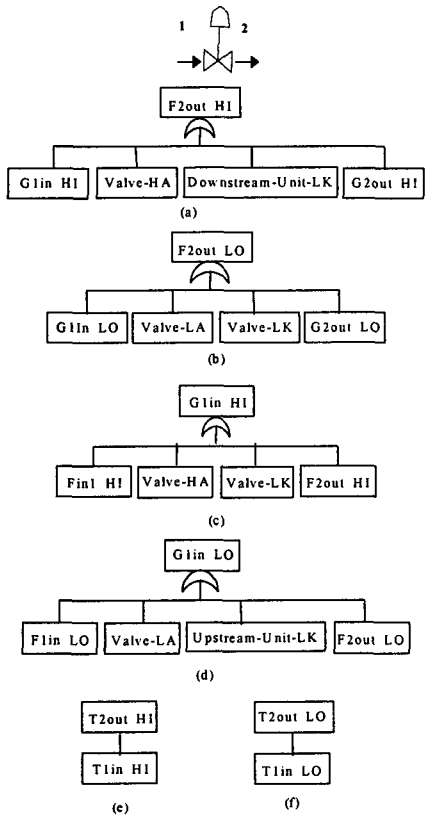

Fig. 5. Valve model

Valve에 대한 전파식은 F2out = f(+G1in, +G2out), G1in = f(+F1in, +F2out), T2out = f(+T1in), X2out = f(+X1in) 등으로 나타낼 수 있다. 따라서 Valve의 출력 2에서의 유량감소 사건과 온도상승사건에 대한 원인-결과 관계를 fault tree형태로 나타낼 수 있다(Fig. 5).

Heat-Exchanger에 대한 전파식은 F2out = f(+G1in, +G2out), G1in = f(+F1in, +F2out), T2out = f(+T1in, -F1in, +F3in, +T3in), X2out = f(+X1in) 등으로 나타낼 수 있다. 따라서 Heat Exchanger의 출력2에서의 유량의 이탈에 관한 룰은 Fig. 6과 같은 fault tree로 나타낸다.

Flow-supply Units에 대한 전파식은 F2out = f(+G1in, +G2out), G1in =f(+F1in, +F2out), T2out = f(+T1in), X2out = f(+X1in)등으로 나타낼 수 있다. 따라서 Pump의 출력2에서의 유량의 이탈에 관한 룰은 Fig. 7과 같다.

2.1.3. 장치간 연결관계

각각의 장치들 사이의 연결관계(relation)는 일반적인 장치간의 연결관계를 나타내는 주(main), 제어루프가 있는 제어(control), standby-line과 같은 보조장치가 연결되어 있는 지지(support)의 3가지로 나눌 수 있다. 대상공정의 장치 및 연결상태를 표현하기 위하여 Equipment Name, Equipment Number, Port Number, Relation등의 속성변수를 사용하여 나타낸다. Fig. 8의 Pipe2에 대하여 Table 3에 그 예를 나타내었다. 이것은 Pipe2의 Upstream에 Pump가, Downstream에는 Valve가 주 관계로 연결되어 있음을 나타낸다. Equipment Number는 대상공정의 장치별로 Upstream으로부터 Downstream으로, Port Number는 Upstream에서 Downstream방향으로 주, 제어, 지지 순으로 번호를 매긴다.

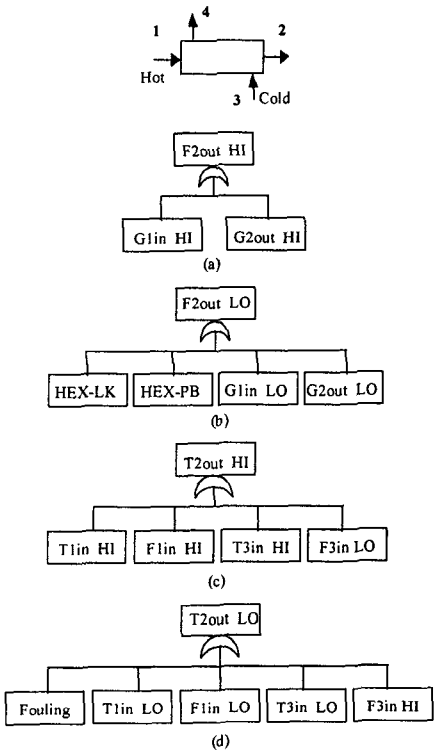

Fig. 6. Heat-exchangers model

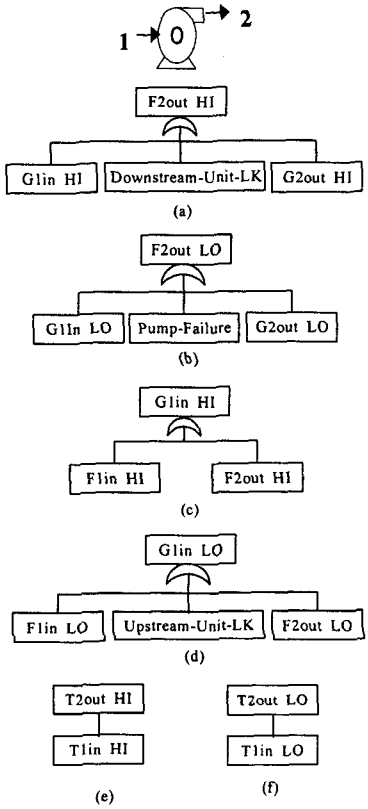

Fig. 7. Flow-supply model

Table 3. Topology representation of Pipe2 in sample system

Equipment Name	Pipe
Equipment Number	2
Upstream Equipment Name	Pump
Upstream Equipment Number	10
Port Number	3
Connected Relation between other components	Main
Downstream Equipment Name	Valve
Downstream Equipment Number	14
Port Number	4
Connected Relation between other components	Main

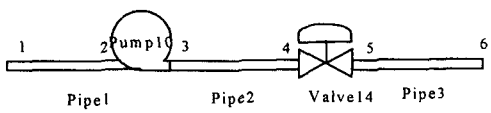

Fig. 8. Sample system

2.2. 장치간 변수이탈 전파(Propagation of Variable Deviation)

화학공정의 어떤 한 장치에서 공정 변수의 이탈이 발생한 경우, 장치지식베이스의 룰과 장치간의 연결관계에 따라 이탈을 전파하여 FT를 합성한다.

변수이탈의 전파는 임의의 장치가 또 다른 장치와 서로 연결되어 있을 때 이 장치간의 변수의 이탈을 전파하기 위한 룰은 다음과 같이

표현한다.

IF [(장치B의 Upstream에 장치A가 연결되어있다.) 그리고 (장치B의 입력에서 변수의 이탈이 있다.)]

THEN (장치A의 출력에서 변수의 이탈이 있다.)

IF [(장치B의 Downstream에 장치C가 연결되어있다.) 그리고 (장치B의 출력에서 변수의 이탈이 있다.)]

THEN (장치C의 입력에서 변수의 이탈이 있다.)

장치 A, B, C가 연속적으로 연결되어 있을 경우 장치 B에서 이탈이 발생한 경우 그 원인을 찾기 위하여 먼저 일반지식베이스에서 장치 B에 대한 해당 룰을 적용한다. 장치 B에서 룰의 적용으로 탐색된 이탈에 대한 원인은 장치 B의 입력, 또는 출력에서의 이탈로 나타나고 이것은 장치간의 연결관계에 의해 Upstream과 Downstream의 장치 A의 출력, 또는 장치 C의 입력에서의 이탈이 된다.

예를 들면, Fig. 8의 Pipe2 출력에서의 유량의 감소와 같은 사건(F4 LO)에 대한 FT를 합성할 경우, 먼저 Pipe룰을 Pipe2에 적용시킴으로서 시작된다. 룰을 적용하면 원인사건으로는 Pipe2-PB, Pipe2-LK, G3 LO, G4 LO가 그 원인이 되고 G3 LO에 대하여 다시 Pipe룰을 적용한다.

이 경우에는 F3 LO, Pipe-PB, Pump-LK, F4 LO가 그 원인사건이 된다. F3 LO은 Pipe2의 입력에서의 이탈로서 변수이탈 전파룰에 의하여 Pump의 출력에서의 이탈이 된다. 이제 F3 LO에 대하여 Pump룰을 적용하여 그 원인을 탐색한다. G4 LO은 Pipe2의 출력에서의 이탈로서 변수이탈 전파룰에 의하여 Valve의 입력에서의 이탈이 된다. 마찬가지로G4 LO에 대하여 Valve룰을 적용하여 그 원인을 탐색한다. 이 경우에는 F4 LO, Valve-LA, Pipe-LK, F5 LO가 그 원인이 된다. 이와 같은 과정을 대상 공정의 경계에 이를 때까지 반복하여 그 원인을 탐색함으로써 FT를 얻을 수 있다(Fig. 9).

2.3. 제어루프의 FT합성

제어루프는 FFLs(FeedForward Loops)와 FBLs(FeedBack Loops)로 나눌 수 있다. FT합성과정에서 제어루프가 있는 경우에는 제어루프가 이탈의 방지 및 억제를 하는 기능이 있으므로 장치간 연결관계가 주(main)관계가 아닌 제어(control)관계일 때의 지식베이스를 이용하여 합성한다. 본 연구에서는 두 가지 형태의 루프에 대하여 장치가 루프를 구성할 때의 이상에 대한 원인-결과 지식베이스를 구축하였으며 이를 이용하여 FT를 합성한다. 루프문제를 해결하기 위한 절차는 다음과 같다.

1) P&ID 상에서 루프의 유무를 확인한 후 이 루프를 구성하는 장치 및 장치간의 연결을

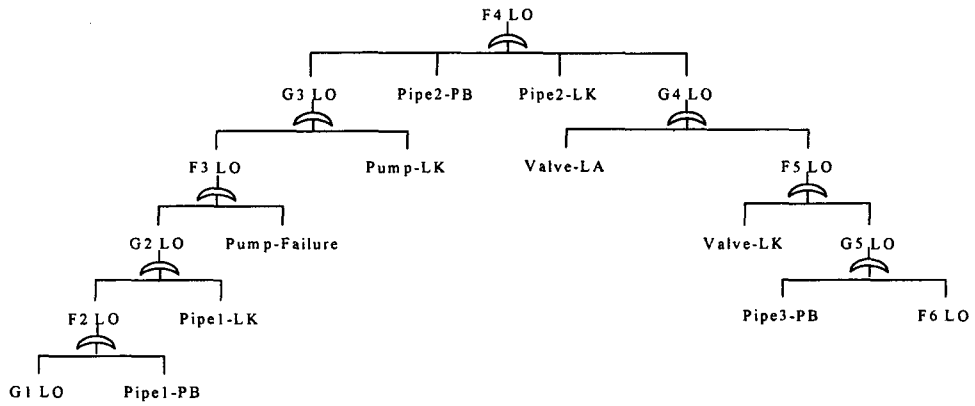

Fig. 9. Fault tree for sample system

확인한다. 2) 루프의 종류를 확인한다(FFLs 또는 FBLs). 3) 루프의 제어변수 및 조절변수를 확인한다. 4) 발생한 이탈에 대하여 제어루프 모델을 적용한다. 5) 적용결과를 검증한다.

루프에서 이탈이 발생하는 경우는 내부외란의 발생, 조절변수의 이탈, 센서가 감지한 변수의 이탈이 발생함과 동시에 루프내의 장치의 비작동으로 인해 적절한 루프의 응답이 없을 경우, 그리고 루프가 제어할 수 없는 변수의 이탈이 발생한 경우 등 4가지로 분류할 수 있다.

내부 외란(internal disturbance)은 루프를 구성하는 장치자체의 고장으로 인하여 이탈이 발생하는 경우이다. 그 예로는 센서의 고장으로 인하여 정상상태인데도 불구하고 이를 정상이 아니라고 판단하는 경우(Sensor failing high)와 제어 밸브가 고장이 나서 닫힌 경우(Control valve failing closed) 등이다. 루프의 비응답(Loop Inaction)은 루프로 제어 가능한 외란이 들어오는 왔음에도 불구하고 루프가 적절한 응답을 행하지 못하는 경우로서 Sensor Stuck과 Control Valve Stuck 등이 그 예가 된다.

3. Case Study

상기의 FT합성과정의 타당성을 검증하기 위하여 간단한 공정에 대하여 적용시켜 보았다. 주어진 공정은 벤젠과 반응하여 질산벤젠을 생성하기 위하여 반응기로 들어가는 뜨거운 질산을 냉각하기 위한 공정으로 이 공정에서 발생할 수 있는 위험한 사건으로서는 질산의 온도상승으로 인한 반응기에서의 폭주반응을 예로 들 수 있다(Fig. 10, 11).

따라서 반응기로 들어가는 질산의 온도상승(Pipe4 Temp HI)을 최상위 사건으로 하여 FT를 합성할 수 있다. 이때 적용시킬 최상위 사건 지식베이스의 룰은 IF [(T6in HI) OR (T7out HI) OR (external heat source)] THEN (Pipe4 Temp HI)이다. 여기서는 외부의 열원에 의한 온도상승(external heat source)은 고려하지 않았다.

그 외의 원인사건 중 Pipe4 출력에서의 온도상승(T7out HI)은 공정의 경계에 해당하므로 더 이상 전개하지 아니하고, Pipe4 입력에서의 온도상승(T6in HI)에 대하여 주(main)관계와

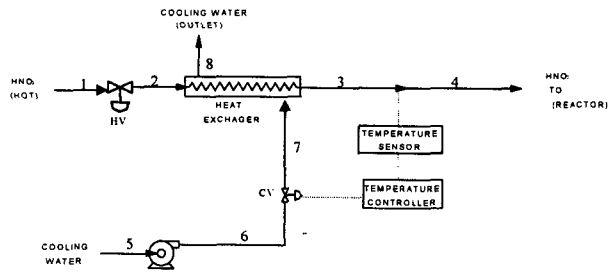

Fig. 10. Nitric acid cooling system

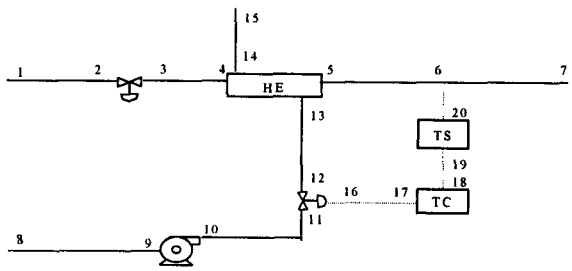

Fig. 11. Block diagram

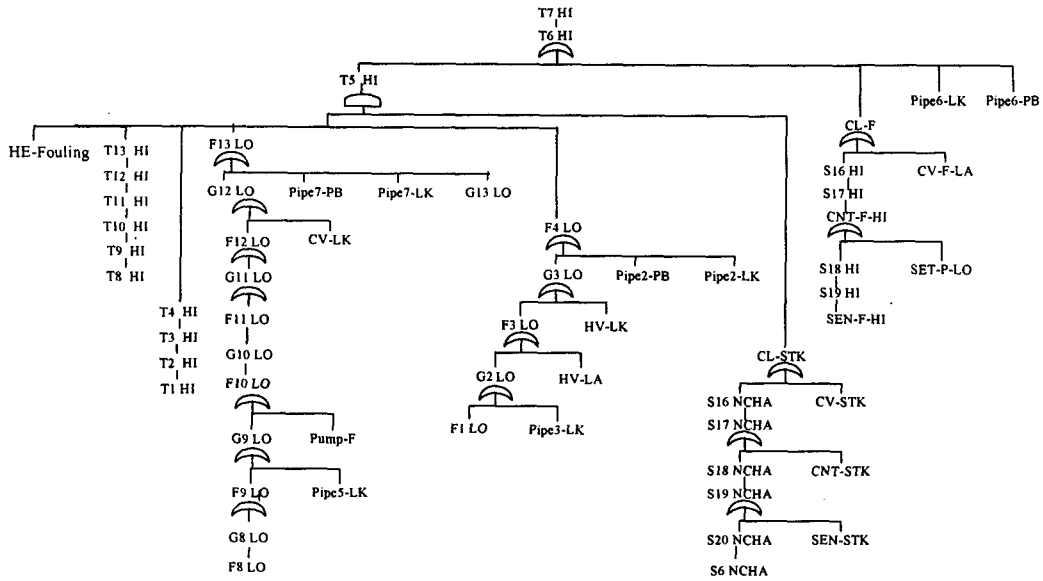

Fig. 12. Automated FT synthesis result

제어(control)관계의 장치지식베이스를 이용하여 이탈전파를 행함으로써 원인사건을 탐색하여 FT를 합성한다(Fig. 12). 기존연구의 결과와 제시된 모델을 적용시켜 합성된 FT의 결과를 비교하여 보면 본 연구에서는 조작자에 의한 이상의 발생은 고려하지 않았으며 Pipe의 leak같은 보다 더 상세한 원인사건을 찾을 수 있음을 알 수 있다.

4. 결 론

본 연구에서는 FT합성 자동화를 위하여 화학공정 장치를 계층적으로 분류하고 변수의 이탈과 장치 이상을 고려한 지식 표현법의 개발하여, 대상공정이 바뀌는 경우에도 지식의 재사용 및 수정을 용이하도록 모델링하였다. 또한 최상위 사건과 장치에 관한 지식베이스 및 장치간의 연결관계 Data를 이용하여 공정변수의 이탈에 대한 양방향 전파를 행함으로써 FT를 자동 합성하였다. 제어루프가 있는 경우에는 루프를 구성하는 장치의 운전상태를 고려한 제어루프 모델을 적용하여 FT의 선명성을 증가시켰다.

참 고 문 헌

1. Lapp, S.A and Powers, G.J., "Computer-Aided Synthesis of Fault Trees.", IEEE Trans. Reliab., 26, 2-20 (1977).
2. Taylor, J.R., "An Algorithm for Fault-Tree Construction", IEEE Trans Reliab, 31, 137-145 (1982).
3. Kelly, B.E. and Lees, F. P., "The Propagation of Faults in Process Plants", Reliability Engineering and System Safety, 16, 3-12 (1986).
4. Carpignano, A. and Poucet, A., "Computer Assisted Fault Tree Construction : a Review of Methods and Concerns", Reliability Engineering and System Safety, 44, 265-274 (1994).
5. Henley, E. J. and Kumamoto, H., "Automated Fault Tree Synthesis By Semantic Network Modeling, Rule based Development and Recursive 3-Value Procedure", Reliability Engineering and System Safety, 49, 171-180 (1995).