

화학공정 안전성평가 기법에 관한 비교 연구

변운섭 · 안대명 · 황규석[†]

부산대학교 화학공학과

(2003. 2. 3. 접수 / 2003. 5. 6. 채택)

A Comparative Study on Safety Analysis Methodology of Chemical Process

Yoon-Sup Byun · Dae-Myung An · Kyu-Suk Hwang[†]

Department of Chemical Engineering, Pusan National University

(Received February 3, 2003 / Accepted May 6, 2003)

Abstract : A new reliability assessment methodology is presented and the new method is compared with fault tree analysis. The system is modeled by directed graph at a new methodology, which is composed of nodes and arcs. The directed graph corresponds to the layout of chemical process and is easy to construct. Therefore, the directed graph analysis is applicable to the chemical process that has complex sequence. The example of fault tree analysis and directed graph analysis is given. The directed graph analysis has proved to be a valuable and useful method for the reliability assessment of chemical process.

Key Words : reliability assessment methodology, fault tree analysis, directed graph analysis

1. 서 론

화학공장은 여러 가지 유해·위험물질을 취급하므로 화재, 폭발 및 위험물 누출사고의 잠재 위험성이 매우 높으나 설계단계에서부터 안전이 고려되므로 사고의 발생빈도는 상대적으로 낮은 편이다. 그러나 사고가 발생할 경우에는 대형사고로 발전되기 쉽고, 사업장의 인적·물적손실 뿐만 아니라 인근지역의 설비나 주민들에게까지 위험을 줄 수도 있다.

최근에는 생산설비가 대형화, 고도화, 복잡화되어 가고 있으므로 그들 설비에서 사고가 발생할 경우 생산의 장기중단이 불가피하고, 설비복구에 따르는 손실과 환경 훼손에 의한 손해배상 뿐만 아니라, 사회적 기업 이미지의 손상 등 직·간접적인 손실이 극심한 실정이다. 특히 우리나라 화학공장의 경우 60년말부터 조성되어 10년 이상된 노후설비가 대부분을 차지하고 있어 사고 위험성은 계속 증가하고 있으므로 설비 노후로 인한 사고를 미연에 예

방하기 위해 공정설비에 대한 적절한 정량적평가를 통한 설비의 정비·보수가 필요하다.

따라서 최근에는 정량적 위험성평가에 대한 연구가 활발히 진행되고, 여러 분야에서 많은 위험성평가 방법들이 개발되고 있다. 그러나 대부분의 위험성평가 방법들이 결정론적 방법을 주로 사용하고 있어 시스템이 어느 정도 신뢰도를 가지고 있는지 그리고 그 신뢰도로 인한 위험성의 증가·감소의 효과가 어느 정도 인지를 정확히 분석할 수 없는 상태이다. 특히, 현재까지 보편적으로 사용하고 있는 결함수분석(Fault Tree Analysis)¹⁾은 현대기술의 발전으로 산업규모의 확대와 함께 복잡한 동작을 가진 대규모시스템이 나타남에 따라 한계에 부딪쳐 새로운 신뢰성평가 기법 도입이 필요하게 되었다.

따라서 본 연구에서는 성공확률을 추구^{2,4)}하는 유향그래프를 이용한 새로운 신뢰성평가 방법을 제시하고, 새로운 기법과 기존의 안전성평가 기법인 FTA에 대한 비교 연구를 통하여 새로운 기법의 장점 및 적용 가능성을 검증하였다. 또한 유향그래프분석 방법을 이용한 신뢰성평가를 통하여 시스템의 정비·보수시점을 추적 관리하고, 시스템의 신뢰도를 일정

[†]To whom correspondence should be addressed.
kshwang@pusan.ac.kr

수준이상으로 유지하면서 보수 및 정비일정의 최적화를 이루어 중대산업사고 예방은 물론 시스템의 효율적인 관리 및 운전 가동률을 향상시켜 기업의 생산성 향상에 기여할 수 있는 방법을 제시하고자 하였다.

2. 결함수분석(FTA)

결함수분석(Fault Tree Analysis)은 정량적 위험성 평가 기법으로 연역적 방법 또는 Top-down 접근방법으로 가장 널리 사용되어 왔으며, 연역적 사고방식으로 시스템의 고장 및 사고를 결함수 차트(Fault tree chart)로 탐색해 나감으로써 고장 및 사고의 원인이 어떤 것인지를 찾아내는 해석기법이다. 본 기법은 1962년 미국의 벨전화연구소의 Watson에 의해 고안된 후 항공우주분야, 원자력분야, 화학공장 등 산업시스템의 안전성평가기법⁵⁾으로 널리 이용되고 있으나 다음과 같은 문제점을 가지고 있다.

2.1. 사상의 적출

Fault Tree에 포함되는 원인사상은 해석자의 생각이 미치는 범위이고 일어날 수 있는 모든 사상을 나타낼 수 없다. 시스템이 복잡해지면 논리적 사고에 의한 원인사상을 적출하는 데는 한계가 있으며 또한 이제까지 알려지지 않았던 미지의 원인이나 현대의 기술범위를 넘는 새로운 현상을 분석하는 경우는 대처할 수 없다.

또한 잠재하는 사고결과는 여러 가지이며 이들 모두를 예측하는 것은 곤란하다. 과거의 사고사례를 조사하면 기기의 고장으로 발전하는 사고결과는 유추되지만 조작자가 플랜트 이상을 알고 이것을 정상으로 복귀시키려고 취한 일련의 조작이 결과적으로 사고를 진전시키는 요인으로 바뀔때는 결과가 너무 여러 갈래에 걸쳐 있기 때문에 적출이 곤란하다. 또한 시스템이 복잡해짐에 따라 과거에 경험하지 못한 사고의 발생 가능성은 높아지며 특히 자동화시스템의 이상에 의한 사고결과를 적출하는데 한계가 있다.

2.2. Fault Tree 작성

Fault Tree의 작성에는 대상시스템의 충분한 이해와 불명확한 사상을 인과관계로 명확화 하는 해석이 사전에 필요하다. 이 검토 작업을 빠뜨리지 않고 확실하게 하기 위해서는 대상에 관한 넓은 지식과

경험이 필요하다. 또한 단순한 인과관계로 복잡한 시스템을 표현하여야 하므로 FTA기법에 대한 상당한 지식이 필요하며 비전문가가 본 기법을 적용하는 데는 어려움이 있다.

따라서 복잡한 시스템을 Fault Tree로 표현할 경우 작성자에 따라 Fault Tree가 다르게 작성될 수 있어 분석의 일관성⁶⁾이 결여될 수 있다. 즉, 같은 공정이라 하더라도 해석자 또는 해석시점에 따라 Fault Tree가 다르게 작성되어질 수 있으며 이로 인하여 정량계산에 있어서도 다른 결과가 도출되어 정량적 데이터로서 유용성이 떨어질 수 있다.

그리고 공정의 상태량처럼 온도, 압력, 유량 등이 상호 간섭적으로 영향을 주는 현상을 AND와 OR의 간단한 인과관계로 표현하기 위해서는 많은 어려움이 있다. 특히, 복잡한 대규모시스템을 이러한 단순한 논리로 표현함에 따라 표현될 수 없는 논리에 대해서는 간과할 수 있으며 또한 이러한 간과로 인하여 나타나는 결과는 예측할 수 없으므로 도출된 결과의 신뢰성이 떨어질 수 있다.

2.3. 사상의 설정

정상사상의 설정은 대상 시스템이나 설비에서 바람직하지 못한 중대한 사상을 설정하게 되는데, 해석목적에 달성하는 범위에서 이후의 해석을 예측하여 결정하여야 한다. 부적절한 설정은 이후의 작업을 쓸데없이 많게 하거나 해석을 불가능하게 하는 경우가 있다. 또한 성공확률을 추척할 수 없고 시스템의 고장을 정상사상으로 설정함에 따라 시스템의 완전한 파괴가 아닌 즉, 바람직한 것으로부터 이탈에 대해서는 예측할 수 없어 예방점검에 활용할 수 없다.

또한 Fault Tree의 사상 설정시 개인차가 많이 나타나는 것은 중간사상의 사고방식이 많은 자유도를 갖고 있으며, 대상시스템을 어떻게 파악하는가에 따라 또는 해석자의 능력에 따라 차이를 나타내기 때문이다. 특히, 시스템이 복잡할 수록 발생 가능한 중간사상의 누락이 증가하게 되며 결과적으로 정상사상 확률의 잘못된 결과를 도출할 수 있게 된다.

2.4. 범용성

해석대상 공정의 변경시 기존 Fault Tree를 이용하여 새로운 시스템을 해석하는데 어려움이 있다. 즉, Fault Tree는 정상사상에서 기본사상까지 Tree형식으로 구성되어 있어 시스템 변경은 이 Tree 자체

의 변경을 의미하기 때문에 Fault Tree 전체의 보완이 필요하며 기존 작성되어 있는 Tree를 수정한 새로운 Tree를 작성하여야 한다. 따라서 많은 시간과 경비가 소요되므로 공정이 자주 변경되는 설계단계에 적용하는데 어려움이 있다.

2.5. 정량계산

정량계산을 위해 우선 확보되어야 하는 데이터는 고장률 데이터와 Human Error 데이터이다. 그런데 이러한 데이터 확보에 한계가 있으며 이로 인하여 도출된 확률의 신뢰성이 떨어진다. 또한 기본사상은 발생이 서로 독립적이고 종속성이 없는 것으로 정량화 계산을 행하는데 실제 전력, 냉각수 등 유틸리티는 이것이 고장나면 시스템내 여러 가지 기기의 기능이 동시에 상실되므로 서로 독립적이지 못하고 종속적이라고 할 수 있다. 따라서 공통모드로서 기본사상 계산은 통계적인 데이터나 유사시스템의 경험 데이터를 이용할 수밖에 없는데 이러한 데이터는 짧은 시간에 축적되는 것이 아니라 오랜기간의 운전경험에서 얻어질 수 있으므로 이러한 데이터의 축적이 선행되어야만 정량적 평가가 가능하게 된다.

또한 Fault Tree 작성시 중복사상⁷⁾이 발생할 수 있으며 이를 정리하는데 한계가 있으므로 FTA에 의해 도출되는 정량적 데이터의 신뢰성이 떨어지게 된다. 그리고 화학공정은 시간이 경과함에 따라 고장이 발생할 확률이 증가하는데, FTA분석은 이러한 시간의 경과를 반영할 수 없으므로 시간에 따라 신뢰도가 감소하는 시스템의 경우 정량적 데이터로서 사용하는데 한계가 있다.

3. 유향그래프분석(DGA)

최근 모든 산업분야에 최첨단 신기술이 적극 적용됨에 따라 기존의 단순한 안전 계수를 바탕으로 한 제품의 설계·생산보다는 신뢰성 개념을 도입한 방법이 요구되고 있다. 일반적으로 시스템을 구성하고 있는 부품의 고장률 및 신뢰도는 지금까지 시스템 및 부품이 있는 경우에 대해서만 예측하여 왔다. 이는 지금까지 생산되지 않은 신제품처럼 고장 정보가 충분하지 않은 경우에는 지금까지 사용해 왔던 고장해석 방법으로는 정확한 고장해석을 표현하기 어려운 점이 있다는 것을 나타내고 있다. 이는 기존의 정량적 위험성평가 방법으로는 한계가 있다는 것을 나타내며 새로운 위험성평가 기법의 도입

이 필요하다는 것을 의미한다. 기존의 위험성평가 기법은 사고에 주안점을 두고 접근하였는데, 새롭게 개발된 Directed Graph Analysis는 기존의 방법과는 다른 정상적으로 작동할 확률 즉, 신뢰성에 주안점을 두고 시스템의 신뢰도를 평가할 수 있는 기법이다.

본 기법은 시스템의 성공확률을 평가할 수 있고, 시간경과에 따라 변하는 신뢰도를 평가할 수 있다. 화학공정의 각종 장치를 구성요소와 비구성요소로 구분하여 구성요소를 노드로, 비구성요소를 아크로 표현한 유향그래프로 모델화 하고, 이 유향그래프를 순차적으로 해석하여 전체 시스템의 신뢰도를 예측하는 기법이다. 또한 공정흐름도를 기준으로 각종 장치를 유향그래프모델의 심벌로 그대로 사용할 수 있어 정량적 위험성평가 비전문가도 쉽게 접근할 수 있다.

3.1. 신뢰도와 고장률의 관계

시스템의 신뢰성 척도를 나타내는 신뢰도함수는 신뢰도를 사용시간 t의 함수로 나타낸 것으로써 그 값은 식(1)과 같이 시간 t에서 정상 작동확률을 나타낸다.

$$R(t) = \frac{n(t)}{N} \tag{1}$$

여기서, N는 초기 부품의 총수를 나타내고 n(t)는 시간 t에서의 잔존수를 나타내며, 시점 t까지 고장난 부품의 누적확률은 식(2)와 같이 된다.

$$F(t) = 1 - \frac{n(t)}{N} \tag{2}$$

따라서 $R(t)+F(t) = 1$ 이 되며, 단위시간당 고장률을 나타내는 고장확률밀도함수는 F(t)를 미분하여 식(3)과 같이 된다.

$$f(t) = -\frac{dR(t)}{dt} \tag{3}$$

이때 시점 t와 (t+Δt)시간 사이에 발생한 고장률을 구간고장률이라고 부르며, 이것을 Δt로 나누고 단위시간당 고장률로 환산한 것을 단위시간당 고장률이라 한다. 따라서 단위시간당 고장률은 식(4)와 같이 된다.

$$f(t) = \frac{R(t) - R(t + \Delta t)}{\Delta t \cdot R(t)} \tag{4}$$

순간고장률은 Δt 가 0으로 수렴할때 고장률 극한값이다. 그러므로 순간고장률을 고장률함수라고 부르며, 이것을 $\lambda(t)$ 로 나타내면 식(6)과 같이 된다. 따라서 신뢰도함수 $R(t)$ 는 식(7)과 같이 되며, 만약 고장률이 사용시간에 관계 없이 일정할 경우 식(8)과 같이 단순화 할 수 있다⁸⁾.

$$\lambda(t) = \lim_{\Delta t \rightarrow 0} \frac{R(t) - R(t + \Delta t)}{\Delta t \cdot R(t)} \quad (5)$$

$$\lambda(t) = \frac{1}{R(t)} \cdot \left[-\frac{d}{dt} R(t) \right] = \frac{-R'(t)}{R(t)} \quad (6)$$

$$R(t) = \exp\left[-\int_0^t \lambda(t)dt\right] \quad (7)$$

$$R(t) = \exp[-\lambda t] = e^{-\lambda t} \quad (8)$$

3.2. 신뢰도 예측 방법

화학공정은 펌프, 반응기, 열교환기 등 구성요소와 배관, 계장신호 등 비구성요소로 구성되어 있다. 구성요소는 조작이 가능한 작동요소와 작동요소를 조작한 결과 기능을 수행하는 기능요소로 구분할 수 있으며 이를 유향그래프로 모델화 할 경우 작동노드와 기능노드로 모델화 된다. 또한 비구성요소는 유향그래프의 아크로 표기하며, 아크는 신호를 가지고 있는데 이 신호강도가 공정의 신뢰도를 나타낸다.

화학공정은 장치를 노드로, 배관을 아크로 표현한 유향그래프로 모델화 되며, 노드는 Fig. 1과 같이 시간경과(T)와 신호강도를 가진 아크로 표현된 주입력신호(S), 부입력신호(P) 및 출력신호(R)의 세가지 입·출력 신호로 연결되며 주입력신호와 부입력신호로부터 각 노드에 따라 다른 출력강도를 발생시키며 이 출력강도가 공정의 신뢰도를 나타낸다. 따라서 이 유향그래프를 순차적으로 해석하여 전체 화학공정의 신뢰도를 예측할 수 있다.

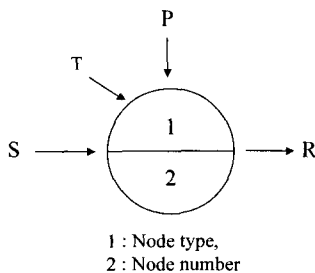


Fig. 1. Symbol of node.

또한 본 기법에서는 각 장치의 동적인 상태에 따라 노드를 구분하므로 화학공정의 동적인 특이인 대기중 보수, 대기중 고장, 기동실패, 운전중 고장등을 평가할 수 있고, 시간에 따른 신뢰도 변화를 예측하므로 화학공정의 적절한 정비·보수시점 예측을 통한 예방점검을 실시할 수 있는 신뢰도 데이터를 제공한다.

4. 사례적용

4.1. 대상공정

본 연구에서는 Platforming Unit의 Net Gas Compressor을 대상공정으로 선정하여 기존의 정량적 위험성평가 기법인 FTA와 새롭게 개발한 DGA를 적용하여 두 기법을 비교·분석하였다. 본 예제에 사용된 Gas Compressor는 수소를 고압으로 압축하므로 가스가 누출될 경우 고압분출화재 등 중대산업 사고가 발생할 가능성이 높으므로 설비의 지속적인 관리가 필요하다.

본 공정에는 3대의 Compressor가 설치되어 있으며 다단으로 수소를 압축하는 Centrifugal Type Compressor이다. Compressor가 정상적으로 작동하기 위해서는 Lube Oil System, Cooling System 등 부속 설비가 정상적으로 작동하여야 하는데 본 연구에서는 이러한 Utility관련 설비는 Compressor Failure에 포함시켜 Fig. 2과 같이 단순화 하였다. 즉, 기존의 정량적 위험성평가기법인 FTA와 새로운 기법인 DGA의 분석결과를 비교하기 위해 공정을 단순화하여 Fig. 2와 같은 흐름도로 나타내었다. 따라서 본 예제에서는 Compressor system 주공정의 온도가 상승하는 경우 온도를 감지하여 경보를 울리고 또한 온도가 계속 상승할 경우 자동이나 수동으로 Compressor를 정지시키는 시스템으로 한정하여 비교를 실시하였다.

전체 Compressor system의 신뢰도를 정확히 예측하기 위해서는 관련 Utility, 전기설비 등 부속설비에 대한 신뢰도를 먼저 예측하여 Main compressor system에 신호를 발생 시키므로써 전체 Compressor system의 신뢰도를 예측할 수 있다. 즉, Sub-System의 신뢰도를 예측한 후 점차적으로 Main-System의 신뢰도를 예측하는 순차적인 방법을 사용하면 전체 시스템의 신뢰도를 예측할 수 있다.

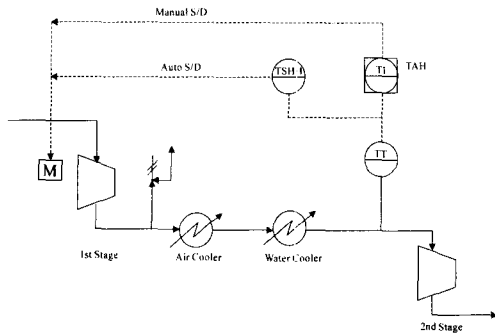


Fig. 2. Compressor system.

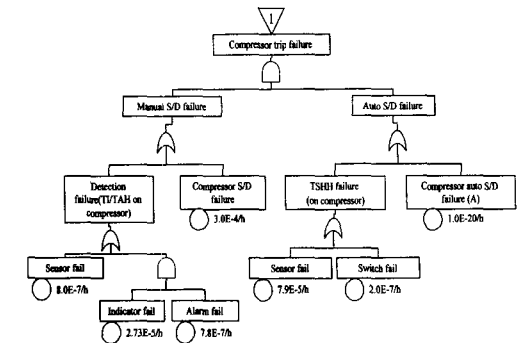


Fig. 4. Fault tree of compressor system (II).

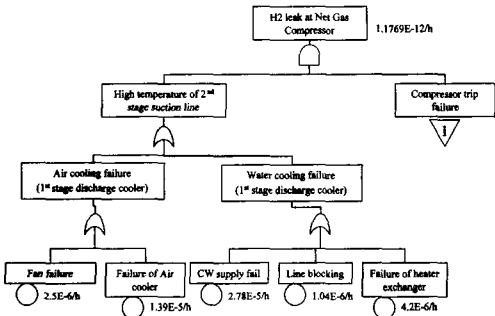


Fig. 3. Fault tree of compressor system (I).

4.2. Fault Tree Analysis 적용

본 공정에 대한 FTA의 적용에 있어 Air Cooler 또는 Water Cooler의 실패로 2nd Stage Suction 온도가 상승하면 Flange가 팽창하여 수소가 누출되면서 외부점화원 또는 누출시 발생한 정전기에 의한 화재 발생을 Top 사상으로 설정하였다. 이러한 Top사상에 대한 Fault Tree는 Fig. 3,4⁹⁾과 같다.

FTA를 이용하여 정량적 위험성평가를 실시하였을 경우 예측된 고압분출화재가 발생할 확률은 1.1769E-12/h로 예측되었다. 그러나 본 기법의 정량적인 결과에는 다음과 같은 가정이 포함되어 있으므로 정량적인 데이터로 신뢰성이 떨어진다. 즉, 수소가 분출될 경우 반드시 화재가 발생하는 것은 아닌데 화재가 발생한다고 가정하였다. 또한 Air Cooler와 Water Cooler중 1개가(OR GATE)가 Failure 될 경우 온도가 상승하는 것으로 가정하였는데 Air Cooler가 효율을 향상시킬 목적으로 설치되어 있을 경우는 다른 결과를 도출할 수 있다. 그리고 온도가 상승할 경우 Flange에 Leak가 발생한다고 가정했으나 주공정의 냉각시스템이 고장날 경우 Flange에 Leak가 발생할 정도로 온도가 상승할 가능성은 낮을 수 있다.

따라서 어떤 사고의 개념보다 시스템의 의도된 운전조건을 이탈하는 것을 정의할 필요성이 있는데 이를 위해서는 시스템의 신뢰도 예측이 필수적이다. 시스템의 신뢰도 예측을 통하여 운전조건을 이탈을 예측하는 방법으로는 DGA방법이 유용할 것으로 판단된다.

4.3. Directed Graph Analysis 적용

본 시스템은 운전중에 신뢰도 감소를 예측하는 것으로 초기 운전시의 실패확률을 제외시키고 의도된 운전조건을 이탈할 경우 Compressor를 정지시키는 경우에 대해 시스템의 신뢰도를 예측하였다. 즉, Cooling System 및 Shut Down System은 시간이 경과함에 따라 정상적으로 작동할 신뢰도가 감소되므로 Cooling System이 정상적으로 작동할 신뢰성과 만약 Cooling System이 고장날 경우 Shut Down시스템이 정상적으로 작동할 신뢰성을 함께 평가하여 Compressor system에 이탈이 발생하더라도 사고로 발전하지 않을 신뢰성을 예측하였다.

신뢰도 해석은 FTA와 비교할 목적으로 Cooling System과 Shut Down이 동시에 Failure되지 않을 신뢰성을 예측하였으며 이를 위해 공정흐름도를 기준으로 Fig. 5와 같이 유향그래프로 모델화 하였다. 또한 기존 FTA시 안전밸브에 대한 사상을 누락하였으므로 DGA에서도 안전밸브를 유향그래프의 모델에 포함시키지 않고 모델화 하였다.

본 시스템의 신뢰도해석 고장률 데이터는 FTA에서 사용한 고장률 데이터를 사용하였다. 또한 시간의 경과에 따른 영향을 예측하기 위하여 0, 100, 200, 300, 4400(0.5년), 8760(1년), 43800(5년)시간에서의 신뢰도를 예측하였으며 여기서 0시간은 최초 운전시점을 나타낸다.

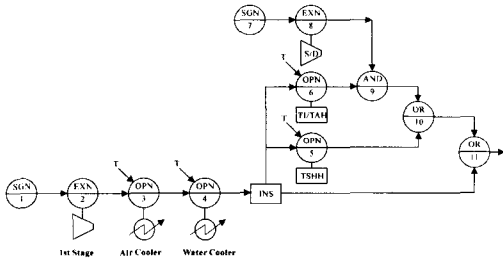


Fig. 5. Directed graph of compressor system.

Fig. 5에서 노드의 상부 기호는 노드의 물리적 의미를 나타내며, 하부 숫자는 노드의 번호를 나타내는데 각 노드의 출력강도를 시간에 따라 순차적으로 계산하여 최종 출력강도를 계산하였다. 이 최종 출력강도(노드 11번)가 본 시스템의 시간에 따른 신뢰도를 나타낸다.

본 시스템 해석에서 FTA기법과 비교하기 위해 시간에 따라 신뢰도가 감소하는 노드 1 즉, Compressor는 모든 시간에서 정상적으로 작동한다고 가정하고 신뢰도를 예측하였으며 수소는 계속 충분히 공급되고 있다고 가정하였다. Fig. 5에서 SGN는 신호발생노드, EXN는 확장노드, OPN는 운전노드 그리고 OR, AND는 논리노드를 나타내는데 각 노드의 의미와 출력강도는 다음과 같다.

4.3.1. 신호발생노드

이 노드는 SGN(Signal generation node)로 나타내며 작동노드에 작동신호를 발생시키는 역할을 수행하는데 입력신호 없이 출력신호를 발생한다. 즉, 수소가 충분히 공급될 경우 노드 1은 "1"의 신호를 발생시키며, Human error를 고려하지 않을 경우 노드 7의 출력강도는 "1"이 된다.

또한 각종 계장시스템에서는 주입력신호가 존재할 경우 신호발생노드를 이용하여 주입력신호로 "1"을 발생하므로 공정흐름도를 기준으로 한 유향 그래프 모델을 작성하기 위해 신호발생노드는 생략한다. 따라서 계장시스템의 주입력신호강도가 "0"이 아닐 경우 주입력신호는 "1"이 된다. 즉, 노드 4의 출력강도가 존재할 경우 노드 5,6의 주입력신호는 "1"이 된다.

4.3.2. 확장노드

이 노드는 EXN(Expansion node)로 나타내며 시스템의 확장성을 고려하여 정의한 노드이다. 단순한 기기 장치를 포함하여 복잡하지만 표준화된 프로세

스를 단일 노드로 정의하므로 공정흐름도를 유향그래프로 모델화 할 경우 공정을 단순화 할 수 있다. 본 시스템에서는 Compressor 및 Shut Down시스템의 작동상태를 본 노드를 이용하여 모델화 하였으며 정상작동 확률(P_g)이 필요하며 출력강도는 식(9)과 같다.

$$R(t) = P_g \cdot S(t) \tag{9}$$

4.3.3. 운전노드

이 노드는 OPN(Operation node)로 표기하며 시스템 운전중 즉, 주입력신호 $S(t)$ 가 존재할 때 장치의 고장을 모델화 한다. 1개의 주입력신호와 시간의 경과를 나타내는 "T"로 부터 1개의 출력신호를 발생시킨다. 이것은 단위시간당 장치의 고장률(λ)이 필요하며 고장률이 시간에 독립적인 것으로 가정할 경우 출력강도는 식(10)와 같다.

$$R(t) = S(t) \exp\{-\lambda \cdot \sum_{k \in t} T_k(t_k) \times \min[1.0, S(t_k)/S(t)]\} \tag{10}$$

4.3.4. 논리노드

화학공정의 기능요소와 작동요소를 유향그래프로 모델화 하는 경우 각 노드를 논리적으로 접속하여야 하는데 이를 접속하기 위해 OR, AND gate가 필요하다.

OR gate는 1개 이상의 주입력신호로 부터 1개의 출력신호를 발생시키며 입력신호에 의해 나타나는 모든 가능성의 합을 얻을 수 있으며 출력강도는 최소한 1개이상의 입력신호가 존재할 가능성을 나타낸다. 입력신호가 서로 독립이면 출력신호의 확률은 식(11)과 같다.

$$R(t) = 1 - \prod_i (1 - S_i(t)) \tag{11}$$

AND gate는 1개 이상의 주입력 신호로부터 1개의 출력신호를 발생시키며 입력신호에 의해 대표되는 가능성의 대표점을 얻을 수 있으며 출력강도는 모든 입력신호가 존재할 가능성을 나타낸다. 따라서 AND Gate는 입력신호가 모두 발생할 경우에 출력신호가 발생한다. 입력신호가 서로 독립이면 출력신호의 확률은 식(12)과 같다.

$$R(t) = \prod_{i=1}^n S_i(t) \quad (12)$$

4.3.5. 신뢰도 예측 결과

Compressor 2nd Suction의 온도가 상승하지 않거나 또는 온도가 상승할 경우 Shut Down이 정상적으로 작동할 신뢰도는 유향그래프모델을 순차적으로 계산하여 최종출력강도로 나타나는데, 본 시스템에서 고압분출화재 등 사고가 발생하지 않을 신뢰도 변화는 Fig. 6과 같이 예측되었다. 본 시스템은 300시간 후 신뢰도가 급격히 감소하는 것으로 나타났다. 따라서 화학공정의 신뢰도를 일정수준 이상으로 계속 유지하기 위해서는 300시간 이후에는 적절한 예방점검이 필요할 것으로 판단된다.

4.4. 평가결과 비교

기존의 FTA은 시간의 경과를 반영할 수 없으며 이탈이 발생할 경우 사고로 발전한다는 전제 조건 하에서 평가가 이루어 졌다. 또한 비전문가가 접근하기 어려우며 본 예제에서와 같이(안전밸브를 시스템 분석시 누락시킴) 사상을 누락할 경우 다른 결과가 도출될 수 있다. 그러나 Fig. 6과 같이 DGA는 시간의 경과에 따른 신뢰도 변화를 나타낼 수 있다. 본 기법의 분석 결과는 사고로 발전하는 고장뿐만 아니라 생산에 영향을 줄 수 있는 정상상태 이탈사항을 포함하고 있어 공정에 대한 HAZOP 등의 정성적 위험성평가 결과 발생하는 이탈에 대한 정량적 평가가 가능하다. 따라서 사업장에서 활용할 경우 과학적으로 점검주기를 예측할 수 있어 생산성 향상에 기여할 것으로 기대된다. 또한 공정흐름도를 기준으로 유향그래프모델을 표현하기 때문에 설비

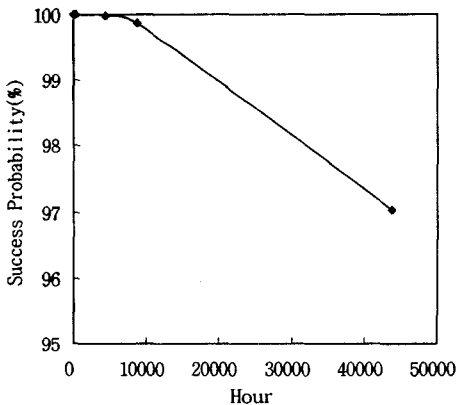


Fig. 6. Success probability in compressor system.

를 누락시킬 우려가 낮으며 비전문가라도 기본적인 노드를 이해하면 누구나 쉽게 접근할 수 있다는 장점이 있다.

본 예제에서는 현재까지 정량적 위험성평가 기법으로 광범위하게 사용되고 있는 FTA와 비교하기 위한 목적으로 유향그래프모델 작성시 냉각시스템의 기능과 Shut Down 시스템을 조합하였다. 그러나 본 기법을 이용하여 정량적 평가를 실시할 경우 시스템이 정상적으로 작동할 확률과 의도된 설계조건을 이탈할 경우 안전장치가 정상적으로 작동할 확률을 각각 분리하여 평가할 수 있다. 즉, 주공정에 대한 의도된 목적을 달성할 수 있는 신뢰도를 해석할 수 있다. 또한 설계 상·하한을 이탈할 경우 공정을 정상적으로 Shut Down시키는 등 안전장치가 정상적으로 작동할 신뢰도도 예측할 수 있다.

따라서 위에서 언급한 것처럼 주공정에 대한 신뢰도 해석을 통하여 일정한 신뢰도 이하가 될 경우 사전에 설비 보수·점검을 통하여 신뢰도를 향상시킬 수 있기 때문에 설비고장으로 인한 경제적 손실을 사전에 예방할 수 있다. 또한 시스템을 안전하게 운전하기 위해 안전관련 시스템의 신뢰도 분석을 실시하여 적절한 점검주기 및 안전설비 추가 등을 결정할 수 있는 정량적인 데이터를 얻을 수 있다. 이러한 관점에서 본 공정을 DGA기법을 이용하여 정량적 위험성평가를 실시하면 다음과 같다.

4.4.1. 주공정에 대한 신뢰도 평가

주공정에 대한 의도된 운전조건으로 운전될 신뢰도를 평가하기 위해 본 시스템을 유향그래프로 모델화 하면 Fig. 7과 같다.

본 시스템 해석에 필요한 각 단의 Compressor 가동중 고장률은 $2.26E-4^{10)}$ 로 가정하였으며 수소를 취급하므로 배관 및 차단밸브의 막힘, 안전밸브의 사전 열림, Human error 등은 고려하지 않고 각 노드별 시간에 따른 출력강도를 계산하여 시스템이 정상적으로 작동할 신뢰도를 예측하여 보면 Fig. 8과 같다. 따라서 본 기법을 이용할 경우 신뢰도 데이터를 근거로 하여 정비·보수시점을 결정할 수 있다.

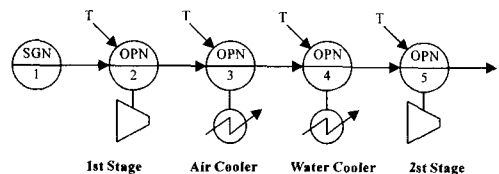


Fig. 7. Directed graph of main system.

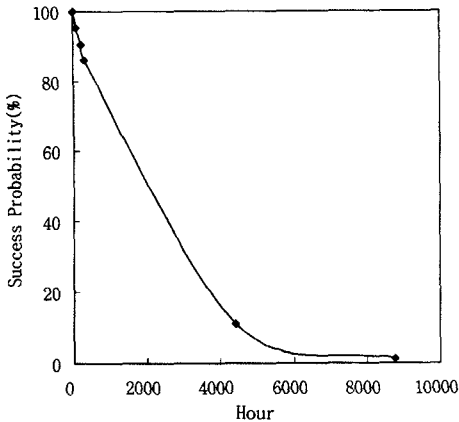


Fig. 8. Success probability in main system.

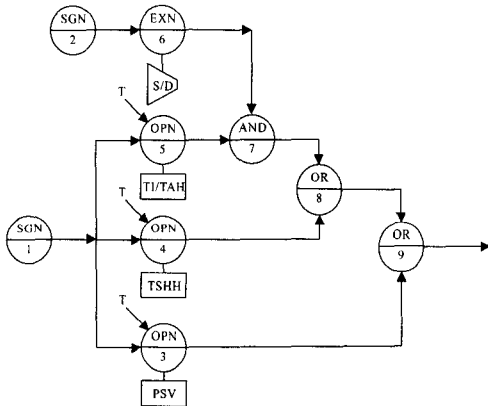


Fig. 9. Directed graph of safety system.

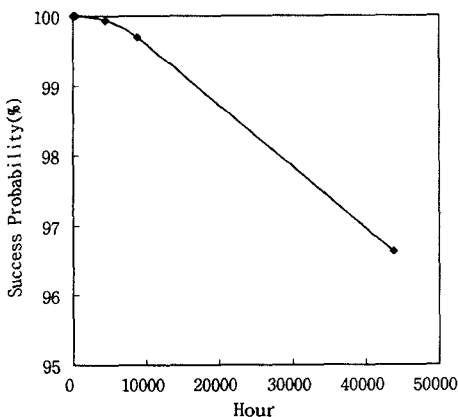


Fig. 10. Success probability in safety system.

4.4.2. 안전시스템에 대한 신뢰도 평가

본 시스템의 안전장치는 안전밸브와 수동 및 자동 Shut Down 시스템이 있다. 이런 안전시스템이

정상적으로 작동할 신뢰도를 평가하기 위해 본 시스템의 안전설비를 유향그래프로 모델화 하면 Fig. 9과 같다.

본 공정의 신뢰도 해석시 필요한 안전밸브의 열림 실패율은 $2.12E-4^{10}$ 로 가정하였으며 Human error는 고려하지 않고 각 노드별 시간에 따른 출력강도를 계산하여 안전시스템의 신뢰도를 예측하면 Fig. 10와 같이 되었다.

따라서 본 기법을 이용하여 화학공정의 신뢰도를 평가할 경우 신뢰도 데이터를 근거로 한 과학적 정비·보수시점을 예측할 수 있어 중대산업사고 예방은 물론 생산성 향상에도 기여할 수 있을 것으로 기대된다.

5. 결론

시스템이 대형화됨에 따라 기존 FTA기법으로 시스템의 안전성을 평가하는데 한계가 있다. 따라서 FTA기법의 정량적 위험성평가 적용시 문제점을 분석하고, 이를 보완한 새로운 DGA기법을 개발하였다. 본 기법은 공정이 복잡하여도 공정흐름도를 기준으로 노드와 아크로 구성된 유향그래프로 공정을 쉽게 모델화 할 수 있어, 정량적 위험성평가 비전문가가도 쉽게 사용할 수 있다. 또한 시스템 변경시 변경된 부분을 보완하여 사용할 수 있어 범용성이 있고, 해석자에 따라 도출된 결과가 거의 일정하므로 정량적 데이터로서 신뢰성을 가지게 된다. 그리고 시간의 경과에 따른 신뢰도를 예측할 수 있어 정비·점검시점을 예측하여 예방점검이 가능하도록 한다.

향후 설비에 대한 고장률 데이터베이스 구축 및 노드의 출력강도를 나타내는 모델식을 쉽게 사용할 수 있는 프로그램을 개발할 경우 기존 공장뿐만 아니라 신규 설계시 활용할 수 있어 정량적 데이터를 근거로 과학적 설계가 가능하다. 또한 본 기법은 화학공장뿐만 아니라 원자력, 전기회로도 등 모든 시스템으로 확대 적용할 수 있으므로 시스템의 신뢰성 평가기술 향상에 기여할 것으로 판단된다.

참고문헌

- 1) 일본종합안전연구소, "FTA안전공학," 기전연구사, 1990.

- 2) T. Matsuoka and M. Kobayash, "Go-Flow : A New Reliability Methodology," Nucl. Sci. Eng., 98, pp. 64-78, 1988.
- 3) T. Matsuoka and M. Kobayash, "The GO-FLOW reliability analysis methodology-analysis of common cause failures with uncertainty," Nucl. Eng. and Des., 175, pp. 205-214, 1997.
- 4) R. L. Williams and W. Y. Gately, "Go Methodology-Overview," Electric Power Research Institute, 1978.
- 5) N. H. Roberts, W. E. Vesely, D. F. Haasl and F. F. Goldberg, "Fault Tree Handbook," NUREG-0492, 1981.
- 6) H. K. Lee, "Study on Digraph Based Fault Tree Synthesis of chemical process," M.D. Dissertation, Pusan National University, 1998.
- 7) Y. M. Kim, "An Algorithm for Risk Analysis using FTA," M.D. Dissertation, Hanyang University, 1996.
- 8) 이치우, 김선진, 이성우, 정상영, "신뢰성공학," 원창추판사, pp. 29-32, 1999.
- 9) 한국산업안전공단, "사고발생확률 분석 시스템 개발," pp. 430-431, 2002.
- 10) 한국산업안전공단, "설비작동에 대한 위험성 해석기법 개발," pp. 141-161, 2003.