SMV를 이용한 보일러의 안전성 평가

박미진 · 이승훈* · 김동운 · 문일
연세대학교 화학공학과 · *(주) LG화학

1. 서 론

보일러는 화학공정 장치 중 플랜트의 열원으로써 공정의 각 요소에서 필요로 하는 스팀을 공급하는 스팀 발생 장치 등 전체 공정에서 중요한 역할을 하고 있다. 따라서 개보수가 계속되어야 하므로 보일러 안전성의 검색이 매우 중요하다.

공정 안전 검색 방법으로 HAZOP, FTA 그리고 전문가 시스템 등이 있다. 하지만 이들 방법들은 공정의 규모가 거대화되어감에 따라 더욱 많은 인력과 시간을 투자해서 수행해야 하며 공정의 개선에 따른 변화가 생길 경우에 처음부터 다시 수행하여야 한다. 이러한 어려움을 극복하기 위해 제안되고 있는 것이 컴퓨터를 이용한 안전성 검증의 자동화이다. SMV는 원래 논리 연산을 위해 개발되었으나 논리 결과의 신뢰성이 높고, 반증 예제 생성 알고리즘으로 인해 안전성 평가에도 응용되고 있다. 안전성 평가시 SMV를 이용하면 모듈화 된 SMV를 이용하여 모델을 세우고 위험한 상황을 검증 질의어를 통해 컴퓨터로 자동으로 검색할 수 있다. 본 연구에서는 보일러에 대하여 SMV의 형태에 맞는 모델을 구축하고 안전성을 검색하였다.

2. SMV의 이용

SMV(Symbolic Model Verifier)는 CTL(Computational Tree Logic)이라는 논리와 BDD(Binary Decision Diagram)를 이용하여 주어진 논리의 참과 거짓을 판별하는 방법이다. 이전의 SMV에 비하여 최근의 SMV는 BDD를 사용하기 때문에 이진 트리(Binary Tree)의 모든 상태(State)를 검색하지 않고 이것을 축소시키거나 반복되는 구간(loop)를 찾아 간략화하여 검색함으로써 10^{120}이상의 상태 수의 검증이 가능하게 되었다.

SMV는 크게 모델을 정의하는 부분과 이것에 의하여 검증 질의어를 검색하는 부분으로 나누어 생각할 수 있다. 화학공정을 정의하여 모델로서 입력하고 이에 의한 안전성을 검색하기 위하여 검증 질의어를 세우게 된다. 이렇게 만들어진 모델과 질문을 검색

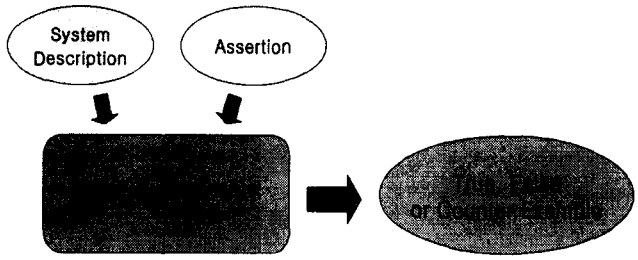
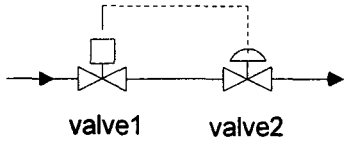


그림1. SMV의 구성요소 및 개요

하여 안전에 관한 검증 질의어가 참인지 거짓인지를 파악하고 거짓일 경우 이에 해당하는 반례를 보여준다. 이러한 결과를 보고 검색 대상에서 위험한 상황이 발생할 수 있는 상황을 찾아내고 이러한 장치의 개선 방안을 수정, 입력하여 이를 다시 검색함으로써 화학공정의 안전성을 향상시킬 수 있다. 이것은 화학공정의 설계시 안전성 검증을 수행할 경우 효과적이며 기존의 공정을 개선할 경우에 안전성을 향상시키는 역할을 할 것이다. 또한 이러한 자동화된 검증법을 사용하는 가장 큰 장점은 모델로 작성된 모든 경우를 검색하여 주기 때문에 사람에 의하여 수행되던 안전성 평가에 비하여 신뢰도를 향상시킬 수 있다는 것이다. SMV 언어로 표현된 밸브 On/Off의 예를 다음에서 보였다.

< 밸브1이 열리면 밸브2도 열린다. >




```
next(valve2) : case
                    (valve1 = 1) :  (valve2 = 1) ;
                    1            :  (valve2 = 0) ;
               esac ;
```

SMV의 보일러 모델

그림 2은 보일러의 공정도이다. 보일러 운전 중 start-up 공정에 있어서 가장 안전사고의 위험이 있는 부분은 보일러의 불꽃을 점화하는 것이라 할 수 있다. 보일러 공정의 start-up을 위하여 먼저 보일러 물 드럼에 물을 공급하고 연료를 예열하여 가열로 안을 퍼지시킨다. 다음으로 연료 공급부에 연료의 누출이 있는지를 검사하고 모든 조건이 만족되면 pilot line에 연료를 공급하여 파일럿 버너를 점화한다. 점화된 파일럿 버너를 이용하여 주버너를 점화하며 주버너 점화 후 순차적으로 연료의 공급을 늘려가게 된다. 이러한 보일러의 start-up은 밸브, 버너, 팬 등의 장치와 연료를 예열, 드럼에 물 공급, 가열로를 퍼지시키는 등의 조작으로 나누어지고 이에 따라 SMV 모델은 각각의 장치나 조작에 관련된 몇 개의 모듈과 수치 연산을 하는 모듈로 구성된다.

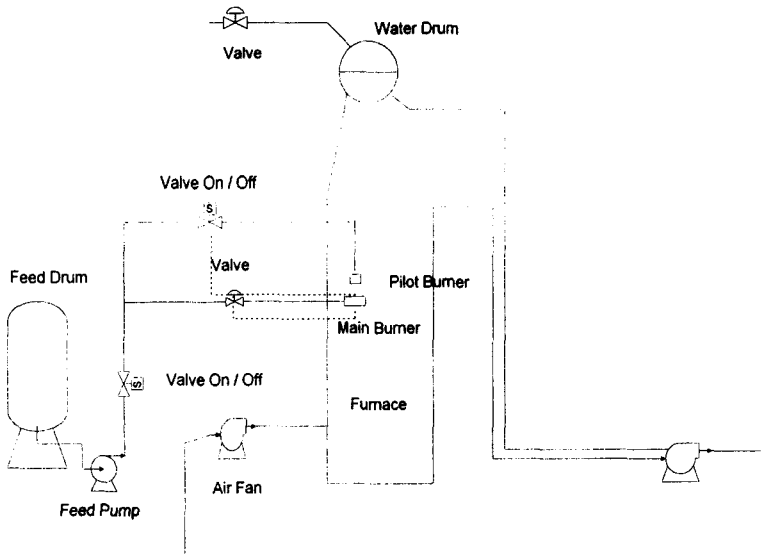


그림2. 보일러의 공정도

SMV의 검증질의어

구현된 보일러의 SMV 모델에 대하여 SMV에서는 검증질의어를 필요로 한다. 검증질의어를 검색하는 것은 SMV에서 자동으로 생성하게 되는 트리를 일정한 순서에 따라 질문의 참, 거짓을 조사하는 것이다. 검증질의어는 구현된 모델의 정확성을 판별하는 기능 검증을 위한 것과 안전 검증을 위한 것으로 나눌 수 있으며, CTL형식을 가지게 된다. 예를 들어, "버너 스타트 버튼이 눌려진 후 버너 내의 불꽃이 감지되지 않으면, 즉각적으로 연료밸브가 닫히는가?" 라는 안전과 관련된 질문이 있을 때, 이것을 검증질의어로 바꾸면 다음과 같다.

AG(StartB -> AF(!BFlame -> AX !CFuel))

여기서 AG는 '모든 경로를 통하여 항상'을 의미하며, AF는 '모든 경로를 통하여 언젠가는'의 뜻이며, AX는 '모든 경로를 통하여 바로 직후에'를 뜻한다. 이런 방법으로 만들어진 질문들은 시스템 모델과 함께 모델 검사기에 입력한다. 모델 검사기는 시스템 모델과 검증 질의어를 받아들여 그림 1에서 보인 것과 같이 시스템 모델이 검증 질의어의 내용에 합당하다면 'true'의 결과를 출력하고, 부적합하다면 'false'의 결과를 나타내고 반례를 보여줌으로써 오류의 위치를 알 수 있게 해주고 시스템의 오류를 수정할 수 있게 도움을 준다.

본 연구에서는 가열로 내의 농도가 일정 수준이상으로 올라가게 되면 점화 시 폭발할 우려가 있으므로 안전 검색을 위한 질문을 "내부의 농도가 일정 농도 이하로 운전되는가" 와 "가열로의 위험한 농도에서 점화원이 존재하는가" 의 두가지로 두었으며 검증질의어는 다음과 같다.

AG(box.conc<9)
=> 가열로 안의 연료의 농도가 기준 이하인가?
AG(ma_detect.sight=1 -> AF(box.conc<9))
=> main burner 점화시 가열로 안의 연료 농도가 기준 이하인가?
AG(pi_detect.sight=1 -> AF(box.conc<9))
=> pilot burner 점화시 가열로 안의 연료 농도가 기준이하인가?

보일러의 조작순서에 따라 먼저 드럼을 채우고 팬을 가동시킨 후 가열로에 오일을 공급하여 버너를 점화하는 순서에 따라 프로그램을 작성하였다. 대부분의 장치는 모듈로 작성하여 버너의 수가 바뀌어도 간단한 과정으로 수정이 가능하고 임의의 장치가 공정에 미치는 영향을 살펴보기 위해서는 그 장치를 나타내는 변수를 non-deterministic variable로 하여 프로그램의 간단한 수정으로 그 장치가 공정에 미치는 영향을 추정해 볼 수 있다.

이를테면 공정중의 팬의 구동이 정상적이지 않을 때는 가열로 내부의 농도가 한계범위를 넘어가게 되는 것을 알 수 있다. 이러한 경우에 개선하여야 할 부분을 SMV프로그램으로 작성하여 보다 안전한 공정으로 가는 방법을 모색할 수 있고 새로운 환경규약등이 제안되는 경우 검증 질의어를 통하여 문제가 될 수 있는 부분의 유무를 확인할 수도 있다. 다음은 팬의 오동작을 SMV 언어로 표현한 것이다.

```
next(running) := case
                    !normal_condition : {0,1} ;
                    1                 : signal ;
                 esac ;
```

팬의 오동작은 주입부 팬의 오동작과 배출부 팬의 오동작으로 나누어 생각할 수 있는데 주입부 팬의 오동작은 가열로 내부의 농도가 위험 수준이상으로 상승할 수 있는 위험을 포함하고 또한 이 상황에서 점화원에 의하여 폭발이 가능하였다. 하지만 배출부

팬의 오동작은 정상적으로 가열로 내부의 농도 조절은 불가능하지만 가열로 내부의 위험한 상황은 발생하지 않았다.

최근의 SMV는 이전의 SMV에 비하여 공정을 보다 세밀하게 표현하는 방법이 발달하여 있고 본 연구에서도 이러한 방법을 이용하였다. 다시 말하면 기존에는 밸브의 On/Off만을 표현하여 왔으나 이것을 밸브의 위치에 따라 여러 단계로 나뉘어 표현하고 이로부터 영향을 받는 변수들도 보다 구체적으로 표현하게 되었다. 이를테면 밸브의 위치에 따른 이전의 SMV의 표현방식은 아래와 같다.

```
next(valve) := case
                 (fan = 1)&(pump_run = 1) : 1 ;
                 1                        : 0 ;
               esac ;
```

위와 같은 표현 방식에서 밸브의 위치를 완전 열림, 반 열림, 닫힘의 형태로 인식할 수 있도록 함으로서 보다 세밀한 표현을 할 수 있다. 이러한 방법의 발달로 실제의 공정에 보다 현실적으로 접근할 수 있다.

```
next(position) := case
                    (position != 0)&(fan = 1)&(pump_run = 1) : position + 1 ;
                    1                                        : 0 ;
                  esac ;
```

3. 결 론

보일러 공정의 start-up 단계의 시스템 모델을 SMV의 양식으로 표현하였고, 보일러 공정의 안전에 관한 질문 사항을 temporal logic을 이용한 검증 질의어로 표현하고 이를 자동으로 검색하였다. 본 연구에서 모델로 선정한 보일러의 경우에 정상적인 조작의 경우 가열로 내부의 농도가 일정 수준이상으로 올라가지 않는다는 결과를 얻어 낼 수 있었고 임의의 장치가 오동작을 할 경우 공정에 미치는 영향을 SMV를 사용하여 확인할 수 있었다. 또한 각각을 소단위로 나누어 모듈화 하였기 때문에 다소 복잡한 공정도 프로그램의 간단한 수정을 통하여 표현이 가능하다. 이렇듯 SMV를 이용하는 것은 기존의 안전 검색 방법과는 달리 정의된 모든 위험성의 발생 가능성을 검색하기 때문에 서로 관련이 없는 장치의 고장에 따른 위험 상황을 효과적으로 검색할 수 있으며 인력과 비용의 측면에서도 많은 이점을 가진다.

참고문헌

1. Moon, I., Automatic verification of discrete chemical process control system, doctorial thesis, Carnegie Mellon University, 1992.
2. Lee, S., Kim, J. and Moon, I., Safety Analysis of Boiler Process Operating Procedures using SMV, HWAHAK KONGHAK, 37(5), pp.679~685, 1999.
3. Il Moon, "Modeling PLCs for logic verification," IEEE Control Systems, 14(2), pp.53-59, 1994.
4. Il Moon, G. J. Powers, J. R. Burch and E. M. Clarke, Automatic Verification of Sequential Control Systems using Temperal Logic, AIChE 38(1), pp.67-75, 1992.