HWAHAK KONGHAK Vol. 37, No. 5, October, 1999, pp. 679-685
(Journal of the Korean Institute of Chemical Engineers)

SMV를 이용한 보일러 공정 운전 절차의 안전성 검색

이승훈 · 김진경 · 문 일†

연세대학교 화학공학과
(1998년 9월 16일 접수, 1999년 5월 26일 채택)

Safety Analysis of Boiler Process Operating Procedures using SMV

Seunghoon Lee, Jinkyung Kim and Il Moon†

Department of Chemical Engineering, Yonsei University
(Received 16 September 1998; accepted 26 May 1999)

요 약

Symbolic Model Verifier(SMV)를 이용하여 보일러 공정의 안전을 검증하는 기법을 개발하였다. SMV는 가능한 모든 경우를 검증하는 자동화된 검증방법을 사용하기 때문에 공정의 모든 변수의 조합, 즉 다중 변수에 의한 공정의 위험상황 발생여부를 검증할 수 있다. SMV를 이용하여 보일러 모델을 구축하고 실제 보일러 공정에서 일어날 수 있는 팬의 고장이나 가열로 내부 불꽃 감지기의 고장과 같은 장치의 오류에 대하여 발생 가능한 위험 상황을 검색하였다. 구축된 모델을 사용하여 논리적으로는 유추하기 어려운 다중 변수에 의한 위험 상황에 대하여 보일러의 안전성을 검증하였다.

Abstract – This study developed an algorithm for analyzing the safety of the boiler system including equipments and operating procedures using SMV(Symbolic Model Verifier). The strength of this algorithm is to verify the interactions of various variables simultaneously, while conventional simulation technique verifies only a few variable at one time. A boiler model is developed using SMV, and it can specify failures of fans, detectors and pumps. This method tests numerous dangerous conditions occurred by multiple variables and identifies potential hazards in the boiler system.

Key words: SMV, Safety Verification, Boiler Process, Operating Procedure

1. 서 론

많은 수의 화학공장들은 건설된지 오래되어 시설이 노후화 되어 있다. 특히 보일러의 경우에는 공정전체의 열원이 되는 중요한 장치로서 개보수가 계속되어야 하므로 안전성의 검색은 매우 중요하다.

화학공정의 안전도와 신뢰도를 평가하는 방법은 매우 다양하다. 이들 중 가장 일반적인 방법은 검사목록표(check list)를 만들어 현장에서 검사하는 것이다. 이것은 복잡하지 않은 공정에 대하여만 사용되고 대규모의 공정에는 방대한 양의 표와 기호를 사용하기 때문에 숙련된 사람의 경우를 제외하고는 사용하기 어렵다. 보다 논리적인 검사방법으로는 변수와 사건들 사이의 논리 관계를 이용하는 방법들이 있다. 가장 대표적인 방법으로는 HAZOP(HAZard and OPerability study)와 FTA(Fault Tree Analysis)가 있다. HAZOP은 공정이 정상 운전 상태에서 벗어난 상태들에 대한 목록을 만들고 이 상태가 발생할 수 있는 경우를 추론하게 된다. 이것은 여러 변수들이나 사건들이 복합적으로 일어나게 되는 경우에는 적용이 어렵다. FTA는 결과로부터 원인을 찾아내는 방법인데 이 방법도 역시 공정 설비와 컴퓨터 소프트웨어 사이에 상호 작용을 검사하는데는 어려운 점이 많다. 먼저 제어 시스템 하드웨어와 운영체계, 응용 프로그램 코드 등이 복잡하면 HAZOP이나 FTA 방식의 위험성 평가 방법으로는 수많은 조합을 검색하기 어렵다. 또한 순차나 배치 공정 시스템에서는 공정과 그 제어계가 가질 수 있는 수많은 상태로 인해 더욱 복잡해진다. 사람에 의하여 수행되는 안전 분석 방법의 단점으로는 공정의 각 변수간의 상호 간섭에 의한 영향을 파악하기가 어려울 뿐만 아니라 시간에 따른 발생 가능한 위험상황에 대한 시나리오의 증가를 감당할 수 없다. 이러한 문제점을 극복하기 위하여 추론 과정을 자동화시킨 안전 검색 기법으로 Symbolic Model Verifier(SMV)를 이용하였다[2].

본 연구에서는 화학공정 장치 중 플랜트의 열원으로서 공정의 각 요소에서 필요로 하는 스팀을 공급하는 스팀 발생 장치 등 전체 공정에서 중요한 역할을 하고 있는 보일러에 대하여 SMV의 형태에 맞는 모델을 구축하고 안전성을 검색하였다. 보일러를 이루고 있는 장치와 공정을 밸브나 연료공급, 펌프, 팬, 퍼지 공정 등의 단위 모듈로 구성하여 보일러의 안전 검색을 위한 모델을 개발하고 개발된 보일러 모델을 이용하여 운전 개시때의 안전성을 평가하였으며 이러한 평가 결과를 보일러의 운전 중에 발생할 수 있는 단일 장치의 고장, 오동작 그리고 고장과 오동작의 조합으로 나누어 발생 가능한 위험상황을 검증하였다.

2. SMV의 이용

SMV는 CTL(Computational Tree Logic)이라는 논리와 BDD(Binary Decision Diagram)를 이용하여 주어진 논리의 참과 거짓을 판

†E-mail : ilmoon@bubble.yonsei.ac.kr

별하는데 이것을 안전에 응용하여 안전에 관한 논리의 참, 거짓을 판별하는데 이용하였다. SMV는 BDD를 사용하기 때문에 이진 트리(binary tree)의 모든 상태(state)를 검색하지 않고 이것을 축소시키거나 반복되는 구간(loop)을 찾아 간략화하여 검색하게 되었다. 이러한 원리를 이용하여 발생할 수 있는 모든 경우를 검색함으로써 논리적으로 유추해내기 어려운 경우라도 모두 검색할 수 있다는 장점이 있다.

Clarke(1986) 등은 모델 기반 검증 방법(Model-based Verification Method)을 개발하였다. 이 방법은 일반적인 이진 연산 논리에 시간의 개념을 표시할 수 있는 연산자가 추가된 형태의 temporal logic을 이용함으로써, 완전한 모사를 위하여 검색하여야 할 공정의 상태 공간의 증대속도를 감소시켰다. Moon(1991) 등은 이산 화학공정 제어 시스템의 안전성과 운전성을 자동으로 검증하는 연구에서 이 검증 방법을 사용하였다. 이 연구에서는 순차 제어 시스템의 안전성을 검증하기 위하여 전체 상태 전이 그래프(State Transition Graph, STG)를 생성한다. 하나의 상태는 유한개의 상태 변수들로 정의되는데, 참이나 거짓의 논리 값을 갖는다. 이 논리 값들로 온-오프 밸브, 펌프, 탱크 수위 등의 이산 상태 값을 나타낼 수 있다. McMillan(1992)은 논리 검증법(Symbolic Model Verification, SMV)을 제시하였는데, 상태의 그래프를 직접 생성하는 대신 이진 표현 식으로 공정 상태들의 집합과 상태간의 전이들을 표현함으로써, 이전의 연구에서 문제점이었던 "상태 폭발 문제(state explosion problems)"를 크게 감소시켰다. 이 방법은 순차이진 결정도(Ordered Binary Decision Diagrams, OBDD)(Bryant, 1987)를 이용하여 이진표현식을 구현하였는데, Burch(1991) 등이 SMV를 사용하여 검증할 수 있는 시스템의 상태 수가 10^{120}이상이 됨을 보였다. Moon(1992)은 SMV를 화학공정에 적용하여 PLC 기반 시스템의 안전성과 운전성을 검증하는 방법을 연구하였다[2, 4]. 이 연구에서 PLC의 RLL(Relay Lader Logic)을 모델로 변환하는 방법을 제시하였고 단위 공정에 대한 모델을 개발하였다. 정(1995)은 이러한 공정 안전성 검증의 자동화를 위한 통합 환경을 X windows 기반의 환경에서 개발하였다[5]. 이것은 사용자 환경을 강조하여 보다 SMV의 사용을 용이하게 하였다. Probst(1996)는 이러한 단위 공정들을 모듈로 표현하여 이러한 모듈들의 조합으로써 전체 공정에 접근할 수 있도록 하였다. 또한 이러한 것들을 고체 운송 체계[1]나 누출 검사, 가열로의 일반적 모델 등에 적용하였다.

Fig. 1에서 Logic Model 부분에는 운전 절차나 장치들간의 관계에 따른 공정 모델 등을 입력한다. Specifications에는 모델의 정확성에 관한 질문과 안전에 관한 질문을 입력한다. SMV는 Specifications의 참, 거짓을 판별하기 위하여 Logic Model에 의하여 자동으로 트리를 합성하고 합성된 트리의 여러 상태들을 검색한다. 검증 결과를 이용하여 안전에 관한 내용을 확인하고 문제가 발생할 수 있는 부분을 파악할 수 있다. 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 효과적이

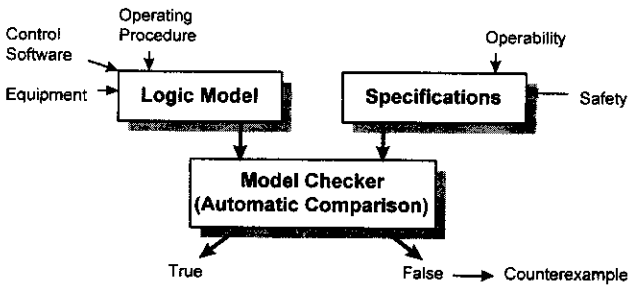

Fig. 1. Structure of SMV.

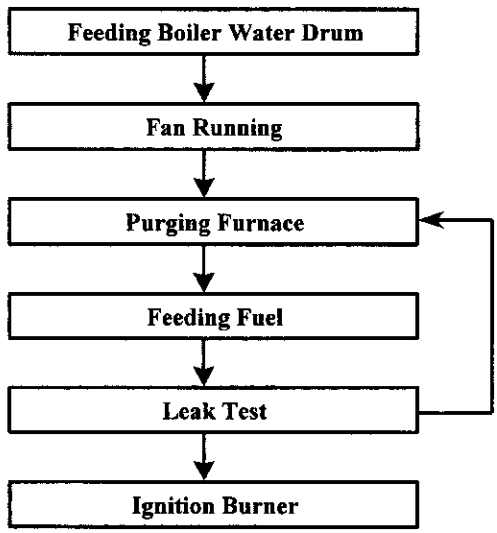

Fig. 2. Operating procedures of boiler.

며 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 있는 장점이 있다.

3. SMV 보일러 모델

3-1. 보일러 공정

SMV를 이용한 보일러 모델의 구현을 위해 설정한 공정 조작의 큰 흐름을 Fig. 2에 나타내었다. 이를 대략적으로 설명하면, 보일러 공정을 위하여 먼저 보일러 물 드럼(boiler feed water drum)에 물을 공급하고 연료를 예열하며 가열로 안을 퍼지시킨다. 이러한 작업후 연료 공급부에 연료의 누출이 없는지를 검사하여 이러한 모든 조건이 만족되면 pilot line에 연료를 공급하여 파일럿 버너(pilot burner)를 점화한다. 점화된 파일럿 버너를 이용하여 주버너(main burner)를 점화하며 주버너 점화후 순차적으로 연료의 공급을 늘려가게 된다. 실제로 주버너의 점화는 torch나 ignitor를 이용하기도 하지만 이들 보다는 자동화된 공정의 검색을 위하여 pilot burner를 이용한 공정을 선택하여 보일러 모델을 구축하였다.

Fig. 3에서 실선으로 표시된 것은 원료, 물, 공기들로써 물질의 흐름을 표현한 것이고 점선으로 표시한 것은 센서에서 나오는 신호의 흐름을 표현한 것이다. 위의 공정도와 Fig. 2의 내용을 기초로 구성하여

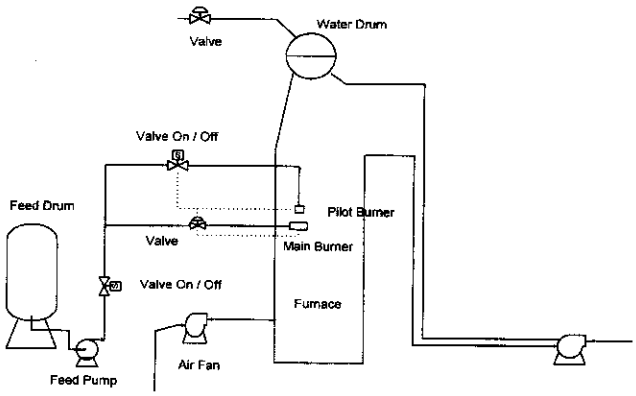

Fig. 3. Flowsheet of boiler.

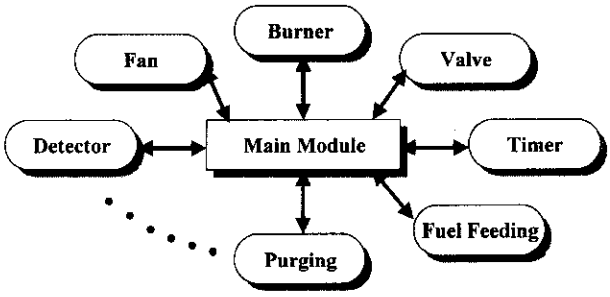

Fig. 4. Structure of SMV modules.

보면 보일러의 start-up은 밸브, 버너, 팬 등의 장치와 연료를 예열, 드럼에 물을 공급, 가열로를 퍼지시키는 등의 조작으로 나누어진다. 이에 따라 작성한 SMV 프로그램은 위에서 나타낸 바와 같이 장치나 조작에 관련된 몇 개의 모듈과 수치적 연산을 하는 모듈 등으로 구성된다.

3-2. 모듈화된 SMV 보일러 모델

대상으로 설정한 보일러 모델에서 각 장치와 그들의 관계를 나타내는 모듈간의 연결을 그림으로 표현하면 Fig. 4와 같다. Fig. 4에서 보는 바와 같이 SMV는 모듈화가 되어 있어 기본적인 형태의 모델을 선정하여 확장이 가능하다. 기본적인 장치에 대한 모듈을 제공함으로써 공정의 조작 조건이 바뀌더라도 기본적인 모듈은 바뀌지 않고 모듈간을 연결시키는 방법만 바꾸어 안전을 검증할 수 있다. 그러므로 본 연구에서는 보일러에서 버너가 1개인 경우를 모델로 설정하였고 일반적인 보일러의 경우 여러 개의 버너로 구성되어 있어도 약간의 수정으로 구현이 가능하다.

3-2-1. 주 모듈(Main Module)

주 모듈에서는 같은 시간 영역에서 각각의 변수가 가지게 되는 값들을 결정해 준다. 이것은 전체 공정의 조작 순서와 장치간의 관계를 규명하여 줌으로서 전체 모델의 가장 큰 흐름을 만들어 준다. 또한 여기서 연결된 하위 모듈(sub-module)의 값들을 받아 이것을 그 상태에서의 값으로 한다. 각각 상태의 흐름은 step이라는 변수와 전체 값들의 변화에 의하여 결정된다. 아래에 pilot 버너와 main 버너에 관하여 연관성의 예를 들었다.

z1pf : burner(step, ignitor.spark, pilot_gas, m1.running)
z1pf : burner(step, z1pf.flame, (p4&(z1b.z>0)), (m1.running& (z1a.z> 0))

여기서 z1pf는 버너의 pilot line이고 z1bf는 버너의 main line이다. 이들 각각은 모듈내부에 점화가 되었는지를 나타내는 flame이라는 변수를 두고 있다. 버너(burner) 모듈은 점화원을 나타내는 spark와 연료를 나타내는 gas, 그리고 공기의 흐름을 나타내는 air의 변수를 필요로 한다. Pilot line에서 점화원(spark)은 ignitor.spark(ignitor의 점화 여부)이고 연료와 공기는 각각 pilot_gas(pilot line으로의 연료 공급 여부)와 m1.running(주입부 팬의 가동 여부)이 된다. 이들 모두가 참인 경우에 burner의 flame이라는 변수가 참이 되고 이것은 z1pf.flame이라는 변수로 지정된다. z1bf는 버너의 main line이고 점화원, 연료, 공기의 흐름은 각각 z1pf.flame(pilot line의 점화 유무), p4&(z1b.z>0)(연료를 공급하는 펌프의 가동유무와 연료를 공급하는 밸브의 열림과 닫힘), m1.running&(z1a.z>0)(주입부 팬의 가동유무와 공기를 공급하는 밸브의 열림과 닫힘)에 대응되게 된다. 이렇게 함으로서 pilot line이 점화(z1pf.flame=1)되면 main line의 점화원으로서 작용할 수 있게 하였다. 다른 여러 모듈들도 위의 예와 같은 유기적인 연관성을 가지고 있다.

```
igniter : spark_plug(in);
z1pf : burner(step, igniter.spark, pilot_gas, m1.running);
z1bf : burner(step, z1pf.flame, (p4 & (z1b.z > 0)), (m1.running & (z1a.z > 0)));
pi_detect : flame_detector(step,preconditions,O03503 , z1pf.flame,normal_pi_detector );
ma_detect : flame_detector(step,preconditions, 1, z1bf.flame,normal_ma_detector);
m1 : fan(step, cont_m1,normal_fan1);
m3 : fan(step, cont_m3,normal_fan2);
m5 : fan(step, !m3.running, normal_fan3);
t100 : very_long_timer(step, t100en);
fuel : fuel_temperature(t100.dn&(z1b.z=0)&(z1p_z=0) );
z1b : valve_position(t100.dn&fuel.temp&purge.On&(step=0)&pi_detect.sight,(t_safety.t=1)|ma_detect.sight , normal_fuel_valve );
z1a : valve_position(m1.running&(step=0), 1 , normal_air_valve );
gas : gas_flow(pilot_gas, p4, z1b.z);
air : air_flow(m1.running, z1a.z, m3.running, door_pos);
box : box_conc(step, air.q, gas.q, (z1pf.flame | z1bf.flame));
purge : purge_process( m1.running&m3.running&z1pf.flame&z1bf.flame, t410.dn,t420.dn);
t415 : retentive_timer(step, t415en, t415res);
t410 : long_timer(step, t410en, t410res);
t420 : retentive_timer(step, t420en, t420res);
t_safety : safety_timer(pi_detect.sight,pgsov2) ;
```

Fig. 5. Main module.

```
MODULE valve_position(normal,interlock , normal_valve)
VAR
z : 0,1,2;
ASSIGN
next(z) :=
    case
            normal_valve :
            case
              interlock :
                        case
                          normal :
                                    case
                                      (z=0) : 1 ;
                                      (z=1) : 2 ;
                                      (z=2) : z ;
                                    esac;
                          1 : 1 ;
                        esac ;
                             !interlock : 0 ;
                             1 : z ;
                        esac;
                1 : 0,1,2 ;
            esac;
```

Fig. 6. Valve position module.

3-2-2. 밸브 위치 모듈

밸브 열림의 경우를 일반화하여 표현하였다. 모듈안에서 밸브의 정상작동의 경우와 오동작의 경우를 결정할 수 있도록 하여 밸브 모듈의 수정 없이 주 모듈에서 변수의 값을 변화시켜 줌으로서 가능하도록 하였다.

3-2-3. 팬 모듈

팬을 가동시키도록 신호가 오면 작동하고 이 경우 역시 모듈내에서 오동작을 구현할 수 있도록 하였다.

3-2-4. 퍼지 모듈

퍼지는 보일러에서 안전을 위해 매우 중요한 조작이다. 대부분의 경우 인털라크가 퍼지 공정으로 향하도록 하고 있으므로 일정한 퍼지를 위한 조건만 되면 바로 모든 밸브를 닫고 퍼지를 하여야 한다. 이것을 퍼지 모듈에서 표현하였다. 여기서 Normal_condition이라는 것

```
MODULE fan(step, signal,normal_condition)
VAR
running : boolean;
ASSIGN
next(running) :=
      case
        !normal_condition : 0,1 ;
        1 : signal;
      esac;
```

Fig. 7. Fan module.

```
MODULE purge_process(normal_condition, timer,timer2)
VAR
On : boolean ;
ASSIGN
next(On):=
      case
            !timer & normal_condition & !timer2 : 0 ;
                                    timer : 0 ;
                                    1 : 1 ;
            esac;
```

Fig. 8. Purge module.

```
MODULE flame_detector(st, hard, soft, flame,normal_condition)
VAR
sight : boolean;
ASSIGN
sight :=
      case
        !normal_condition : 0,1 ;
        !(hard & soft) : 0;
        1 : flame ;
      esac;
```

Fig. 9. Flame detector module.

은 퍼지를 시켜주는 조건을 나타내고 이것은 주 모듈에서 &(and)나 |(or)로 연산된 값을 받아들인다. 하지만 이러한 퍼지 공정은 대부분의 인털락크에 사용되기 때문에 공정에 약간의 오동작이나 오류가 있을 시에도 행하여지므로 경제성의 측면에서 보면 모든 인털락크를 퍼지 공정으로 하는 것은 좋은 효과를 얻을 수 없다.

3-2-5. 불꽃 감지기 모듈(Flame Detector Module)

불꽃 감지기 모듈은 일종의 센서로서 버너가 점화되었는지를 감지하고 신호를 보내 밸브를 열고 닫는다. 주 모듈에서 호출한 방식에 따라 주 버너의 불꽃 감지기로 작동할 수도 있고 pilot 버너의 불꽃 감지기로 작동할 수도 있다.

3-2-6. Timer 모듈

Timer는 주어진 시간에 따라 Very long timer, long timer, retentive timer 등으로 나누었고 이러한 각각의 모듈을 호출하여 주 모듈에서 사용할 수 있다.

3-2-7. 버너 모듈

버너 모듈은 작동에 필요한 불꽃, 연료, 공기의 유무를 받아들여 이들에 대한 조건이 만족하게 되면 점화되었다는 신호를 불꽃 감지기를 통하여 보낸다.

3-2-8. 기타

이 외에도 연료의 흐름을 나타내는 Gas_flow 모듈, 공기의 흐름을 나타내는 Air_flow 모듈, 가열로 내부의 농도를 계산하는 Box_conc 모듈, Ignitor에 점화 신호를 보내는 Spark_plug 모듈, 연료도입부에서 연료를 예열시켜 주는 Fuel_temperature 모듈 등이 있다.

```
MODULE very_long_timer(step, en)
VAR
t : 0..10;
ASSIGN
next(t) :=
        case
          !en      : 0;
          step > 0  : t;
          !(t = 10) : t + 1 ;
          (t = 10)  : t;
        esac;
DEFINE
dn := (t = 10);
```

Fig. 10. Timer module.

```
MODULE burner (step, spark, gas, air)
VAR
flame : boolean;
ASSIGN
next(flame) :=
      case
        !gas : 0;
        !air : 0;
        flame : 1;
        spark : 1;
        1 : flame;
      esac;
```

Fig. 11. Burner module.

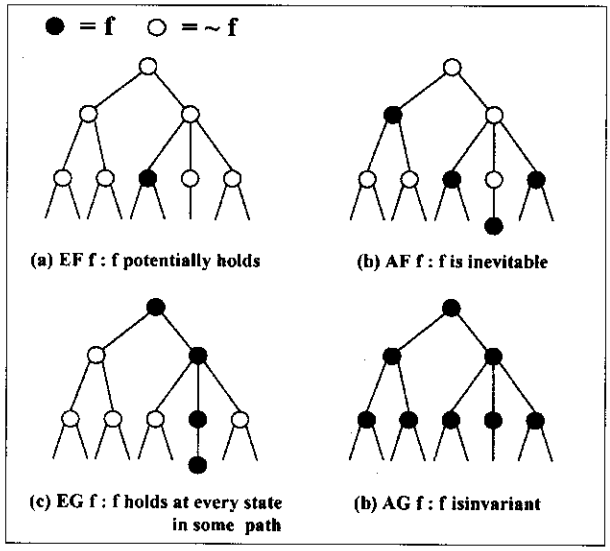

Fig. 12. CTL operator.

4. 검증질의어

구현된 보일러의 SMV 모델에 대하여 SMV에서는 검증질의어라는 것을 필요로 한다. 검증질의어를 검색하는 것은 SMV에서 자동으로 생성하게 되는 트리를 일정한 순서에 따라 질문의 참, 거짓을 조사하는 것이다. 이러한 검증질의어는 CTL의 형식을 가지게 되고 이것에 의한 명제 p가 참이 되는 경우를 Fig. 12에 나타내었고 각각의 의미는 다음과 같다.

(a) EF f : 현재의 상태에서부터 진행되는 상태들 중에서 f를 가지고 있는 상태가 적어도 하나 이상 있다.

(b) AF f : 현재의 상태에서부터 시작하는 모든 경로에서 f를 가지고 있는 상태가 적어도 하나 이상씩 있다.

(c) EG f : 현재의 상태에서부터 시작되는 경로 중에서 그 경로의 모든 상태가 f를 가지고 있는 경로가 존재한다.

(d) AG f : 현재의 상태에서부터 시작되는 모든 경로의 모든 상태가 f를 가지고 있다.

위와 같이 A(all), E(some), F(future), G(globally)로 구성된 연산자를 이용하여 순차적으로 트리를 검색하게 된다.

이러한 검증질의어는 두 가지 형태로 입력하게 되는데 구현된 보일

러 모델의 정확성을 판별하는 기능 검증을 위한 것과 안전을 검증하기 위한 안전 검증 질의어로 나눌 수 있다.

4-1. 기능 검증을 위한 질의어

모델의 정확성을 검증하기 위한 검증질의어는 다음에 설명할 안전을 위한 검증질의어에 정확성을 부여하기 위한 부분이다. 이러한 검증질의어는 대상으로 선정한 모델에 맞추어 SMV 프로그램으로 만든 후 이러한 프로그램이 정확하게 모델링되었는지를 검사한다. 본 연구에서 사용해 보았던 모델을 위한 검증질의어는 정상적인 start-up과 정상운전의 경우에 가열로 내의 버너가 점화되는지를 확인하는 검증질의어와 이러한 과정에서 모델링한 순서대로 장치들이 작동하는지를 결과를 보고 검증하였다. 또한 보일러 안전에 중요한 부분을 차지하는 퍼지 공정에 대하여 일정시간 동안 정확한 조건에서 시행하는지를 검증하였다.

예를 들어 가열로내 버너의 점화 여부를 판별하는 검증질의어는 다음과 같다.

AG(z1b.flame=0)

위와 같은 검증질의어를 검색하는 과정은 다른 변수들이 변화하는 동안 모든 상태에서 버너에 불꽃이 점화되지 않는가를 검색하고 버너가 점화되는 경우 이에 대한 예를 결과로 나타낸다. 이러한 검증질의어에 의한 결과는 모델링한 순서에 맞게 운전 순서를 거쳐 보일러가 점화되는 것을 알 수 있었다.

4-2. 안전 검색을 위한 질의어

정확성이 검증된 모델에 대하여 안전을 검색하기 위한 검증질의어를 입력시켜야 한다. 이때 입력하게 되는 검증질의어는 전체 시스템에서 관심이 있는 부분에 대하여 이를 질문의 형태로 입력시켜 준다. 예를 들어 배관에서 누출이 있는가를 검사하는 경우에는 일정 구간에서 압력의 변화나 유량의 변화를 이용하여 나타내고 고체 수송장치의 경우에는 고체 수송, 저장에 따른 bypass line의 역할에 대하여 나타내면 된다. 본 연구에서는 가열로 내의 농도가 일정 수준이상으로 올라가게 되면 점화시 폭발할 우려가 있으므로 가열로 내부의 농도를 일정 수준이하로 유지하는 것을 안전의 목표로 설정하였다. 또한 이러한 경우에 점화원이 존재하면 바로 보일러의 폭발로 이어지므로 검증질의어를 다음의 두 가지 질문으로 나누었다.

가열로 안의 농도가 안전한 범위 안에서 운전되는지를 묻는 검증질의어와 가열로의 위험한 농도에서 점화원이 존재하는지에 관한 검증질의어로 나누었고 이들을 논리적으로 해석하여 보면 위험한 수준의 농도와 점화원이 없으면 보일러는 점화되지 못하고 계속 퍼지의 과정만 반복되므로 안전은 하지만 경제적인 손실을 가져온다고 나타내었고 위험한 농도와 점화원이 있는 경우는 폭발한다고 가정하였다.

위의 내용을 검증질의어와 그 의미를 다음에 나타내었다.

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

이러한 안전에 관한 검증질의어에 의한 검증의 결과 정상 start-up 상황이나 정상 운전시에 안전한 범위에서 운전되는가를 확인할 수 있었다. 여기서 9라는 값은 설정치로서 상대적인 의미에서 위험한 수준의 농도로 설정하였다.

5. 장치의 오동작에 따른 안전 검색 결과

공정을 이루고 있는 장치들 중에서 안전에 중대한 영향을 미칠 수 있는 장치를 찾아내기 위하여 구성 장치 중 몇 개의 장치에 대하여 오동작과 고장의 상황을 가정하여 안전을 검색해 보았다. 본 연구에서는 앞에서 설명한 모델에 대하여 안전을 검색하고 이를 통하여 발생할 수 있는 위험한 상황이 전개되는 시나리오를 찾아낼 수 있었다. 임의의 장치 고장 상황의 설정을 공기를 불어 넣어주는 팬의 고장과 오동작으로 인한 가열로 내부의 위험 상황의 발생 유무, 또한 pilot detector의 고장과 오동작에 따른 위험 상황 발생 유무를 단일 변수에 의한 영향이라고 설정하였다. 공정 중의 여러 가지 변수의 동시고장, 즉 두 가지 이상의 변수가 동시에 고장을 일으키는 경우에 대하여 안전을 검색하여 보았다. 여기서 고장은 항상 거짓의 값을 갖는 것으로서 팬이 움직이지 않는 상황과 detector가 항상 불꽃이 없다고 신호를 보내는 경우를 나타내고 오동작은 실제 측정값에는 상관없이 참, 거짓 중 임의로 값을 가지는 경우를 나타낸다.

5-1. 단일 변수의 영향과 발생 가능한 위험 상황의 전개 시나리오

5-1-1. 팬의 고장

이 상황은 팬 모듈로 전달해주는 값 중에 Normal_fan1의 값을 항상 거짓으로 하여 사건을 발생시킬 수 있다. 주입부의 팬의 고장과

```
DEFINE
preconditions := 1 ;
iri := 1 ;
O03503 := 1 ;
door_pos :=1 ;
p4 :=1 ;
p6 :=1 ;
t415en := 1 ;
t415res := 1 ;
normal_fan1 := 0 ;
normal_fan2 := 1 ;
normal_pi_detector := 1 ;
normal_ma_detector := 1 ;
normal_fuel_valve := 1 ;
normal_air_valve := 1 ;
```

Fig. 13. Representation of fan failure.

```
MODULE fan(step, signal,normal_condition)
VAR
running : boolean;
ASSIGN
next(running) :=
      case
        !normal_condition : 0;
        1 : signal;
      esac;
```

Fan failure

```
MODULE fan(step, signal,normal_condition )
VAR
running : boolean;
ASSIGN
next(running) :=
      case
        !normal_condition : {0, 1} ;
        1 : signal;
      esac;
```

Fan malfunction

Fig. 14. Comparison of failure and malfunction of fan.

배출부의 팬의 고장으로 나누어 생각해 볼 수 있는데 이들의 경우 팬의 고장으로 인하여 보일러의 점화를 시행하지 않으므로 가열로 내부의 농도가 위험한 수준이상으로 상승하는 경우가 발생하지 않는다.

5-1-2. 팬의 오동작

이 경우는 표현된 형식은 팬의 고장과 유사하지만 의미는 크게 다르다. Normal_fan의 값을 거짓으로 하고 이에 따른 값을 Nondeterministic으로 표현한다. 이것은 {0,1}로 나타내어 해당되는 경우 참이나 거짓 중 임의의 값을 가지도록 하는 것이다. 이것을 Fig. 14에 나타내었다. 이것 역시 주입부 팬의 오동작과 배출부 팬의 오동작으로 나누어 생각해 볼 수 있다. 주입부 팬의 오동작은 가열로 내부의 농도가 위험한 수준이상으로 상승할 수 있는 위험을 포함하고 또한 이 상황에서 점화원에 의하여 폭발이 가능하였다. 하지만 배출부 팬이 오동작은 정상적으로 가열로 내부의 농도 조절은 불가능하지만 가열로 내부의 위험한 상황은 발생하지 않았다.

5-1-3. Pilot Detector의 고장

가열로에 있어서 버너의 점화는 전체 공정을 계속 진행시킬 것인가 또는 처음의 단계로 다시 돌아갈 것인가를 결정하게 되는 중요한 요소이다. 그러므로 pilot detector와 주 버너 flame detector는 고장이나 오동작시에 많은 경제적 손실을 가져오게 된다. Detector의 고장시에는 가열로 내부의 농도가 기준이하로 운전하게 된다는 면에서 안전에 영향은 없으나 점화가 되지 않으므로 공정의 start-up을 계속 진행할 수 없다. 또한 버너가 점화되지 않는 결과를 보이므로 경제적인 손실을 가져오게 된다. 이러한 detector의 고장은 다음의 두 가지로 해석할 수 있다. 버너가 점화되지 않은 경우에 detector에서 점화되지 않았다는 신호가 오는 경우와 점화가 되었는데도 불구하고 detector에서 점화가 되지 않았다고 신호가 오는 경우로 나누어 생각할 수 있다. 앞의 detector의 고장은 안전에 있어서 별 문제가 없다. 왜냐하면 점화가 되지 않으면 퍼지의 공정으로 연결하여 가열로 안의 농도를 안전한 범위 이내에서 운전할 수 있기 때문이다. 하지만 버너가 점화되었는데도 불구하고 detector에서 점화되지 않았다는 신호가 오는 경우에 연료의 공급을 차단하고 퍼지를 하게 되면 공정의 재조작 경우에도 다시 점화가 이루어지지 않았다는 신호를 보내므로 공정이 계속 진행될 수 없다. 또한 이 경우 detector가 고장 났는지 쉽게 알 수 없다.

5-1-4. Main Detector의 고장

이 경우에는 pilot detector에서는 점화 신호가 오고 주버너와 main detector에서는 점화되지 않는 경우이므로 쉽게 파악할 수 있다. 하지만 점화는 시키지 못하고 계속 퍼지하는 경우가 발생하고 이 경우에는 main detector를 수리하여야 한다.

위의 결과를 Table 1에 나타내었다.

이들 중 팬 고장의 경우 보일러의 가열로를 퍼지하기 때문에 가열로가 점화되지 못하고 안전한 범위에서 운전되는 경우를 확인할 수 있었다. 또한 detector의 고장은 보일러의 점화를 성공적으로 수행하지는 못하고 연료의 손실을 가져오지만 안전에 있어서 위험한 상황이

Table 1. Verification results for the single variable

	Safe/ Danger	Ignition of boiler (Success/Fail)	Comparison
Failure of fan(inlet)	Safe	Success	Abnormal operation
Malfunction of fan(inlet)	Danger	Success	Explosion possible
Failure of fan(outlet)	Safe	Success	Abnormal operation
Malfunction of fan(outlet)	Safe	Success	Abnormal operation
Failure of main detector	Safe	Fail	Economical loss
Malfunction of main detector	Safe	Success & Fail	Economical loss
Failure of pilot detector	Safe	Fail	Economical loss
Malfunction of pilot detector	Safe	Success & Fail	Economical loss

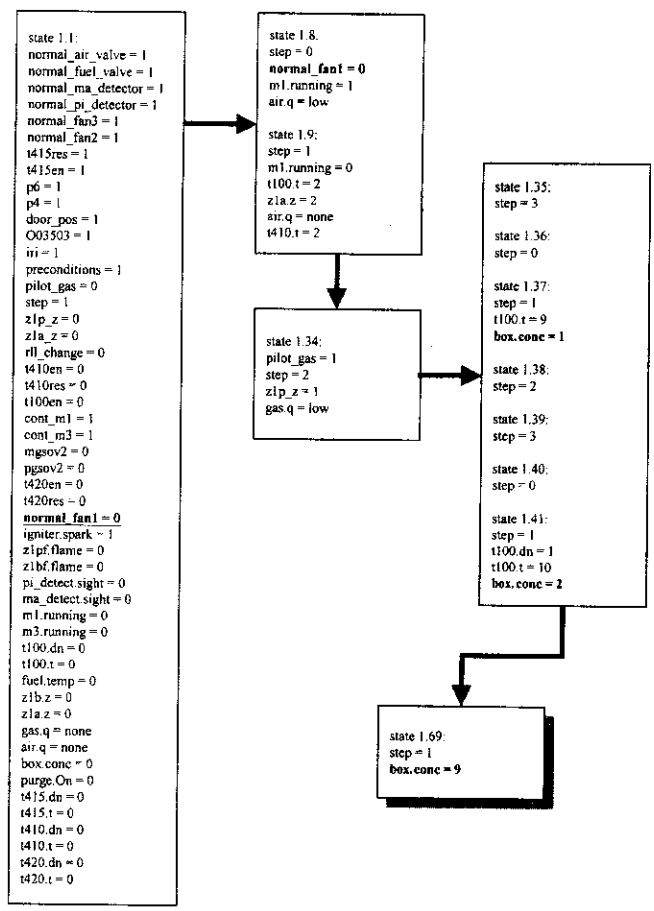

Fig. 15. Scenario for the malfunction of the fan.

라고 할 수 있는 가열로 내부의 농도가 위험 수준 이상으로 상승하는 것은 막을 수 있다. 하지만 주입부 팬의 오동작은 위험한 상황을 발생시킬 수 있었고 발생 시나리오는 Fig. 15와 같다.

5-2. 다중 변수의 영향과 결과 해석

앞에서 임의의 장치 고장에 따른 보일러의 안정성을 검색해 보았지만 여러 장치의 관련 없는 동시 고장이나 오동작은 장치들이 논리적인 연관성을 갖지 않는 경우 추론하기 어렵다. 하지만 연관 없는 장치의 고장과 오동작에 따른 위험 상황 발생여부를 SMV에서는 가능한 모든 경우를 검색하기 때문에 가능하다. 본 연구에서는 앞의 단일 변수의 영향에 의하여 수정된 보일러의 논리 중에서 서로 연관 관계를 가지고 있지 않은 팬과 detector의 고장과 오동작에 대하여 다음의 8가지 경우로 나누어 안전성을 평가해 보았다. 여기서 안전에 관한 질문은 보일러 내부의 농도가 위험한 수준 이상으로 상승하는가와 위험한 수준의 농도에서 점화원이 있는가로 나누어 질문하였고 위험한 수준에서 점화원이 있으면 폭발한다고 가정하였다.

5-2-1. 주입부 팬의 고장과 Pilot Detector의 고장

Pilot detector의 고장으로 점화가 이루어지지는 않는다. 그러므로 가열로 안의 농도가 기준이상으로 상승하여도 폭발은 일어나지 않으나 연료의 공급이 계속 반복되므로 경제적인 손실을 가져온다.

5-2-2. 주입부 팬의 고장과 Pilot Detector의 오동작

팬의 고장으로 연료가 공급되지 못하므로 점화가 발생하는 위험한 상황은 발생하지 않는다. 하지만 pilot line을 통한 연료의 계속적인

Table 2. Verification results for the multiple variables

	Safe/ Danger	Ignition of boiler (Success/c)	Comparison
Failure of fan(inlet) & Failure of pilot detector	Safe	Fail	Economical loss
Malfunction of fan(inlet) & Malfunction of pilot detector	Danger	Success	Explosion possible
		Fail	Economical loss
Failure of fan(inlet) & Failure of main detector	Safe	Fail	Economical loss
Malfunction of fan(inlet) & Malfunction of main detector	Danger	Success	Explosion possible
		Fail	Economical loss
Failure of fan(inlet) & Malfunction of pilot detector	Safe	Fail	Economical loss
Malfunction of fan(inlet) & Failure of pilot detector	Safe	Fail	Economical loss
Failure of fan(inlet) & Malfunction of main detector	Safe	Fail	Economical loss
Malfunction of fan(inlet) & Failure of main detector	Danger	Success	Explosion possible
		Fail	Economical loss

공급으로 인하여 경제적인 손실을 가져온다.

5-2-3. 주입부 팬의 오동작과 Pilot Detector의 고장

Pilot Detector의 고장으로 점화가 이루어지지 않으므로 계속적인 연료의 손실을 가져오게 된다.

5-2-4. 주입부 팬의 오동작과 Pilot or의 오동작

팬이 정상운전의 신호를 보내고 pilot line뿐만 아니라 main line을 통하여도 연료가 공급되고 팬이 정상적으로 운전되지 않으면 가열로 내부의 농도가 위험수준까지 상승한다. 점화가 되지 않았다는 신호를 보내던 pilot detector가 점화가 되었다는 신호를 보내게 되면 main burner가 작동하고 점화원에 의하여 점화가 가능하여 진다. 그러므로 이러한 상황으로 전개시에는 보일러의 폭발이 일어난다.

5-2-5. 주입부 팬의 고장과 Main Detector의 고장

팬의 고장으로 연료의 공급이 이루어지지 않고 main detector의 고장으로 점화가 이루어지지 않으므로 위험한 상황은 발생하지 않는다.

5-2-6. 주입부 팬의 고장과 Main Detector의 오동작

팬의 고장으로 연료의 공급이 이루어지지 않으므로 폭발의 상황은 발생하지 않는다.

5-2-7. 주입부 팬의 오동작과 Main Detector의 고장

팬이 정상운전의 신호를 보내고 pilot line뿐만 아니라 main line을 통하여도 연료가 공급되고 팬이 정상적으로 운전되지 않으면 가열로 내부의 농도가 위험수준까지 상승한다. 이 순간 pilot burner에 의하여 점화되면 폭발할 수 있다.

5-2-8. 주입부 팬의 오동작과 Main Detector의 오동작

팬이 정상운전의 신호를 보내고 pilot line뿐만 아니라 main line을 통하여도 연료가 공급되고 팬이 정상적으로 운전되지 않으면 가열로 내부의 농도가 위험수준까지 상승한다. 이 순간 pilot burner에 의하여 점화되면 폭발할 수 있다.

위의 결과를 Table 2에 나타내었다.

6. 결 론

SMV를 이용하는 것은 기존의 안전 검색 방법과는 달리 정의된 모든 위험성의 발생 가능을 검색하기 때문에 서로 관련이 없는 장치의 고장에 따른 위험 상황을 효과적으로 검색할 수 있다. 이것을 이용하여 공정의 장치들 중 보일러에 대한 모델을 세우고 구성 장치의 고장과 오동작에 따른 안전을 검색하여 보았다. 단일 변수에 의한 영향으로 팬, 주 감지기 그리고 조 감지기에 대하여 고장과 오동작으로 나누어 안전을 검색하여 보았고 이들 중 공기 주입부 팬의 고장은 보일러가 폭발할 수 있는 위험한 상황이 발생할 수 있다는 것을 알 수 있었다. 또한 다중 변수에 의한 영향은 팬, 주 감지기, 조 감지기의 고장과 오동작의 조합으로 구분하여 안전을 검색하였고 이 경우는 팬의 고장, 오동작이 감지기의 고장, 오동작과 동반된 경우에 보일러가 폭발 가능하다는 것을 확인할 수 있었다.

감 사

본 연구는 연세대학교의 재정적 지원으로 이루어졌으며, 이에 감사드립니다.

참고문헌

1. Probst, S. T., Powers, G. J., Long, D. E. and Moon, I.: *Comp. Chem. Eng.*, **21**(4), 417(1997).
2. Moon, I., Powers, G. J., Burch, J. R. and Clarke, E. M.: *AIChE*, **38** (1), 67(1992).
3. Moon, I.: *IEEE Control Systems*, **14**(2), 53(1994).
4. Moon, I., Ko, D., Probst, S. T. and Powers, G. J.: *J. of Chem. Eng. of Japan*, **30**(1), 13(1997).
5. Jeong, S. H., Lee, K. S. and Moon, I.: *Journal of Control, Automation and Systems Eng.*, **2**(1), 53(1996).