VIS 검증기를 이용한 FBD 명세의 정형검증

신모범°, 유준범, 차성덕
한국과학기술원 전자전산학과 전산학전공
{mbshin, jbyoo, cha}@dependable.kaist.ac.kr

Formal Verification of FBD specification using VIS Verifier

Mo Bum Shin, Junbeom You and Sungdeok Cha
Dept. of EECS, Div. Of CS, Korea Advanced Institute of Science and Technology

요 약

원자력 발전소의 제어 시스템은 safety-critical 소프트웨어로서 안정성이 중요시 되는 시스템이다. 최근 기존의 시스템이 PLC 기반의 디지털 제어장치로 대체되면서 이에 사용되는 소프트웨어의 안정성과 품질을 보장하기 위한 정형검증 기법이 요구되고 있다. 특히 PLC 프로그램의 설계에 사용되는 FBD의 모델체킹을 통한 정형검증에 대한 연구는 미비한 수준이다. VIS 검증기는 위의 요구에 부합하는 도구로서 이를 사용하면 여러 종류의 정형 검증이 가능하다. 본 논문에서는 VIS를 이용한 FBD의 검증을 위해서 FBD를 Verilog로 변환 하는 기법을 제안한다. 제안하는 방법의 효율성을 검증하기 위해서 현재 KNICS 사업단에서 개발중인 APR-1400용 원자로 보호 시스템의 운전정지회로를 예로 사용하였다.

1.서 론

원자력 발전소의 제어기는 안전성이 중요시되는 시스템으로서, 제어기에 사용되는 소프트웨어는 높은 수준의 품질을 요구한다. 최근 원자력 발전소의 시스템이 PLC기반의 디지털 제어 장치로 대체되고 있다. 따라서 PLC 소프트웨어 개발 초기 단계에서 품질과 안전성을 보장하기 위한 정형검증 기법이 요구되고 있으며 이를 지원하는 도구의 필요성이 증가하고 있다. 정형기법은 원자력 발전소의 안전성 검증에 큰 역할을 하여 왔다. 예를 들면 정형기법의 하나인 SCR[1]은 한국과 캐나다의 원자력 발전소의 노심제어기의 명세 작성에 사용되었으며 또한 KNICS 컨소시엄의 ARP-1400 노심보호시스템의 명세에 NuSCR[2]이 사용되었다.

PLC는 실시간 제어장치에 널리 사용되는 산업용 컴퓨터의 한 종류이다. IEC(International Electrotechnical Commission)[3]에서는 PLC를 위한 프로그래밍 언어를 정의하고 있으며 그 중 FBD(Function Block Diagram)는 디자인의 정확성에 높은 수준의 신뢰성을 제공하기 때문에 프로세스 제어장치의 설계에 널리 사용되고 있다. 이런 장점으로 인하여 KNICS에서는 소프트웨어의 디자인 명세에 FBD를 사용하고 있으며, 규제기관에서는 FBD의 엄격한 안정성 입증을 요구하고 있다.

VIS 검증기는 여러 검증기법을 수행할 수 있는 통합도구로서 원자력 발전소의 제어시스템의 안전성 보장을 위해 큰 역할을 할 수 있을 것으로 기대된다. 이를 사용하여 두 개의 FBD 프로그램이 같은 동작을 하는지에 대한 동치 검사를 수행 있으며, 또한 모델 체킹을 사용하여 시스템이 특정 속성을 만족하는 지에 대한 검사를 할 수 있다.

본 논문에서는 원자력 발전소의 제어시스템 소프트웨어의 정형검증을 위해서 FBD를 VIS의 입력 언어인 Verilog[4] 프로그램으로 변환하는 기법을 제시하고 있다. VIS 검증기를 이용하면 FBD프로그램을 보다 효율적으로 검증할 수 있다. FBD의 의미를 정확하게 반영하는 변환을 위해서는 FBD의 실행 순서를 유지할 뿐만 아니라 FBD의 일부분이 아닌 전체 시스템의 설계를 고려해야 한다.

논문의 추후 구성은 다음과 같다. 2장에서는 FBD와 VIS, 그리고 VIS의 입력이 되는 Verilog 프로그램에 대하여 소개한다. 3장에서는 FBD의 VIS 입력으로의 변환의 예를 살펴보고 이를 KNICS APR-1400 RPS 명세의 적용한 사례를 소개한다. 마지막으로 4장에서는 본 논문의 결과와 발전 방향에 대하여 언급하겠다

2. 배경지식

2.1 Function Block Diagram

FBD는 PLC 어플리케이션상에서 컴포넌트간의 많은 양의 데이터 흐름을 표현하기 위해서 널리 사용되는 프로그램이다. 회로를 구성하는 제어 컴포넌트 사이의 정보의 이동을 function block의 네트워크를 사용하여 설계할 수 있으며, 시스템의 동작을 신호의 흐름을 통해 표현한다.

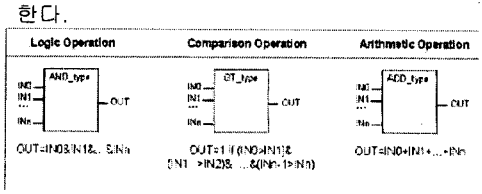

그림 1 NPP 디지털 소프트웨어에 사용되는 IEC63131-3 FBD 예제

Function Block은 다른 Function Block의 입출력 변수와 연결되며, circuit diagram을 통해 Block 간의 관계를 시각적으로 표시한다.

2.2 VIS (Verification Interaction with Synthesis)

VIS는 정형검증, 시뮬레이션 그리고 유한 상태 하드웨어 시스템의 합성을 지원하는 통합도구이다. 외부와의 인터페이스를 위해 Verilog 프로그램의 전단부를 사용하여 Computational Tree Logic(CTL) 모델 체킹, Language emptiness checking, combinational and sequential 동치검사(equivalent checking), cycle-based simulation 과 hierarchical synthesis를 수행한다.

Verilog 프로그램은 직접회로 설계에 널리 사용되는 Hardware Description Language이다. 디자인의 초기단계에서 다른 하드웨어 상에서의 시험과 정확성 검사를 위해 널리 사용되고 있으며 VIS의 입출력을 위한 인터페이스로 사용된다.

3, FBD 프로그램의 정형검증

본 장에서는 FBD의 정형검증을 위해 FBD를 VIS의 입력인 Verilog 프로그램으로의 변환하고 VIS의 다양한 기능들을 이용하여 정형검증을 수행한 결과를 소개한다. Verilog로의 변환과정에서는 여러 변환 규칙이 사용되어야 하며, 본 논문에서는 KNICS APR-1400 RPS 명세의 VIS 입력으로의 변환 사례 중심으로 소개한다.

3.1 Verilog 프로그램으로의 변환

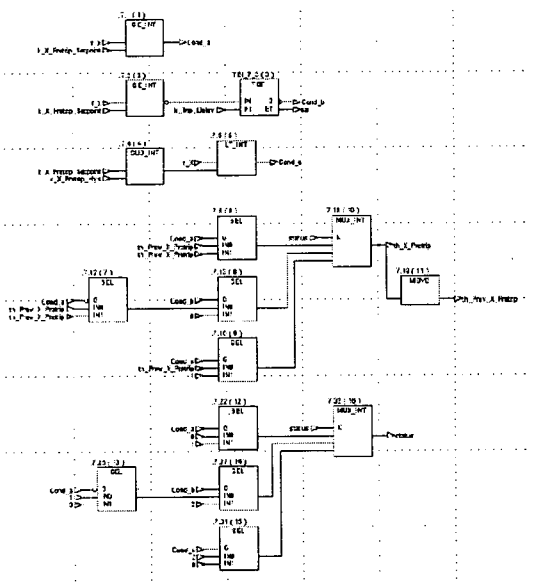

그림 2 고정설정치상승트립 FBD

그림 2 는 원자로 제어기의 운전정지회로인 고정설정치상승트립의 일부분이다. 입력변수(f_X)가 고정 설정치(k_X_Pretrip)를 일정시간(k_Trip_Delay)동안 초과하면 k_X_Pretrip을 0으로 설정한다. 이는 원자로가 동작을 멈추어야 하는 상황을 의미한다.

[그림2]의 상단 FBD는 매크로와 같은 기능을 수행하는 부분으로 출력변수인 Cond_a, Cond_b, Cond_c에 대한 중복 연산을 전처리를 통해서 줄이게 된다. 첫 번째 블록의 Cond_a는 입력 변수(f_X)와 고정설정치를 비교하여 입력변수가 큰 값을 가지면 1 반대의 경우에는 0을 갖는다. 두 번째 블록의 경우, 일정시간(k_Trip_Delay) 동안 입력변수(f_X)가 고정설정치 값을 초과하는지에 대한 결과값을 Cond_b로 출력한다. 마지막 블록에서는 입력변수(f_X)와 고정설정치(k_X_Pretip_Setpoint)에서 미리 설정된 히스테리시스(k_X_Pretrip_Hys)를 감소시킨 값을 비교하여 그 결과를 Cond_c에 저장한다.

중단의 FBD는 Cond_a, Cond_b와 Cond_C를 입력으로 받아 현재 상태를 반영하는 th_X_Pretrip변수를 출력한다. status 는 하단의 MUX_INT function block에 의해 결정되며 현재의 상태를 반영하는 th_X_Pretrip를 출력한다.

```
module Output_Processing (clk, in1, in2, in3, in4, out);
 input clk;
 input in1;
 input in2;
 input in3;
 input [0:1] in4;
 output out;

 reg th_Prev_X_Pretrip;
 initial th_Prev_X_Pretrip = 1;

 assign out = MUX_INT(in4,  SEL(in1, th_Prev_X_Pretrip, th_Prev_X_Pretrip),
    SEL(in2, SEL(!in1, th_Prev_X_Pretrip, th_Prev_X_Pretrip), 1'b0),
    SEL(in3, th_Prev_X_Pretrip, 1'b1));

 always @(posedge clk) begin
   th_Prev_X_Pretrip = out;
 end

 function SEL;     //function SEL definition
   input in1;
   input in2;
   input in3;
   begin
     SEL = (in1 == 1)?in3:in2;
   end
 endfunction

 function MUX_INT;     //function MUX_INT definition
   input [0:1] in1;
   input in2;
   input in3;
   input in4;
   begin
     MUX_INT = (in1 == 2'b00)?in2:
          (in1 == 2'b01)?in3:
          (in1 == 2'b10)?in4:0;
   end
 endfunction
endmodule
```

그림 3 FBD의 Verilog 변환 예

그림 2 중단 부분의 FBD를 Verilog 프로그램으로 변환하면 그림 3 과 같다. FBD프로그램이 Verilog의 기본 entry인 모듈로 구현되었으며 5개의 입력 변수와 1개의 출력 변수를 가진다. input과 output 선언은 FBD의 입력변수와 출력변수를 의미한다. assign문을 통해서 출력 변수에 continuous assignment를 하고 있다. 즉 데이터의 흐름이 오른편에서 왼편으로 진행되며 가장 오른편의 함수의 입력의 변화가 왼편의 모든 함수의 출력에 영향을 끼치게 된다. th_Prev_X_Pretrip변수는 후에 PLC 실행에 사용되기 때문에 다음 모듈로 전달될 수 있는 reg 변수로

선언되었다. FBD에서 변수의 사용 시점이 선언보다 늦은 데이터는 reg 형의 변수로 선언이 되어야 한다.

MUX_INT와 SEL 블럭은 함수로 선언되었다. 이들 함수는 모듈 안에서 선언되어야 하고 다른 함수 또는 다른 블록에서 호출이 가능하다. SEL 함수와 MUX_INT 함수에서는 in1 입력 변수의 값에 따라 입력 변수 중 하나의 값을 출력하게 된다. 특히 주의할 점은 SEL 함수가 각각 다른 변수를 입력으로 받아 4번 수행된다는 것이다. out 변수 선언의 경우, FBD의 실행순서를 고려하여야 하며 이는 FBD 프로그램을 Verilog 프로그램으로 변환하기 위해서 고려해야 하는 중요한 요소 중 하나이다. 마지막으로 각각 모듈은 실행 순서에 따라서 함수를 호출하게 된다. 다른 FBD도 비슷한 방법으로 변환이 가능하다.

3.2 FBD의 정형검증

VIS를 사용한 FBD의 검증에는 다음과 같은 2가지 방법이 사용 가능하다. 그 중 하나는 특정 단계의 FBD가 중요 속성을 만족하는지 확인하는 모델 체킹이고 나머지 하나는 2개 이상의 서로 다른 단계에 있는 FBD가 같은 행동을 하는지에 대해 확인을 하는 동치검사이다.

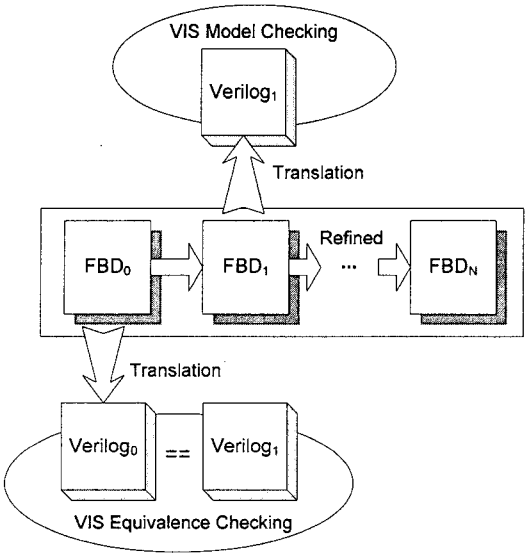

그림 4 FBD에 대한 VIS 정형검증 과정

동치검사(equivalent checking)

VIS 검증기는 두 종류의 동치검사를 지원한다. Sequential 동치검사(equivalent checking)는 시스템 단계의 검사를 수행하며 저장 변수를 포함한 모든 FBD를 대상으로 한다. Combinational 동치검사(equivalent checking)는 컴포넌트 단계 즉 저장 변수를 제외한 FBD의 일부분을 검사한다.

현재 KNICS에 의해 개발중인 APR-1400용 RPS의 공식 프로토타입인 FDB를 대상으로 동치검사를 수행하였다. 여러 syntax 및 logical error가 발견하고 수정할 수 있었다. 결과적으로 VIS를 이용한 FBD의 combinational 동치검사와 Sequential 동치검사는 효율적으로 수행되었다.

모델 체킹

VIS 검증기를 사용하여 CTL Model checking이 가능하다. 시스템이 특정 기능을 만족하는 것에 대한 검사를 수행하는 것으로서 FBD프로그램을 Verilog 프로그램으로 변환하여 VIS의 입력으로 사용하였다.

만약 특정 속성이 만족되지 않는 경우는 반례를 결과값으로 보여주게 된다. KNICS APR-1400에 대한 모델 체킹은 현재 진행 중에 있으므로 중요한 CTL 속성의 분류에 초점을 두고 있다. 물론 핵 공학의 전문가와의 공동 작업이 필요하다

시뮬레이션

VIS는 다른 검증기와 달리 cycle-based 시뮬레이션 수행이 가능하다. 모델 체킹이나 동치검사의 결과를 시뮬레이션의 입력으로 사용하여 반례에 대한 보다 자세한 분석을 가능하게 한다.

4. 결론 및 향후 연구 과제

원자력 발전소와 같이 안전성이 중요시되는 곳에 사용되는 소프트웨어는 작은 오류로 인하여 많은 인명과 재산의 손실을 야기할 수 있다. 따라서 정형기법을 사용하여 개발 초기단계에서 소프트웨어의 결함을 미리 감지하는 방법이 필요하다.

본 논문에서는 FBD를 VIS 입력으로 변환하는 방법을 제안하고 있다. 제안된 방법으로 FBD를 Verilog 프로그램으로 변환하여 효율적인 정형검증을 수행할 수 있었다.

앞으로 제안된 FBD 변환 방법은 KNICS APR-1400 RPS의 실제 구현에 사용할 예정이다.

참 고 문 헌

[1] K. L. Heninger. Specifying software requirements for complex systems: New techniques and their application. *IEEE Trans. Software Engineering*, SE-6(1):2-13, 1980.

[2] Junbeom Yoo, Sungdeok Cha, Han Seong Son, Chang Hwoi Kim, and Jang-Su Lee. PLC-based safety critical software development for nuclear power plants. In *the 23th International Conference on Computer Safety, Reliability and Security (SAFECOMP 2004), LNCS 3219*, pages 155-165 Potsdam, Germany, Sept. 21-24 2004.

[3] IEC(International Electrotechnical Commission). International standard for programmable controllers: Programming languages, 1993. part 3.

[4] D. E. Thomas and P. R. Moorby. *The Verilog Hardware Description Language*. Kluwer Academic Publishers, 1991.