'98 춘계학술발표회 논문집
한국원자력학회

Statechart-based Formalism을 이용한 원전 필수안전 소프트웨어의 자동생성

김장열, 이현철, 정철환, 차경호, 권기춘
한국원자력연구소
305-353 대전광역시 유성구 덕진동 150번지

요 약

본 논문은 David Harel이 제안한 Statechart based Formalism과 Statemate MAGNUM toolset을 이용하여 월성 원전 2/3/4호기 증기발생기 수위로 인한 원자로 정지를 activity chart 및 statechart로 모델링하고 K&R C 코드를 자동으로 생산하였다. 이는 종전의 몇몇 소프트웨어 전문가에 의해서 개발될 수 밖에 없었던 원전 필수안전(Safety-critical) 소프트웨어를 정형화된 Computer Aided Software Engineering 도구를 활용하여 소프트웨어 생명주기중 요구사양명세 및 설계까지만 수행하고 그 이하는 모두 자동으로 생산하는 소프트웨어 공학의 핵심기술을 연구한 것이다. 자동으로 생산된 K&R C 코드는 품질이 우수하고 생산성이 높으며 이식성이 뛰어남을 확인할 수 있었다.

I. 서 론

종래에는 몇몇 숙련된 소프트웨어 프로그래머들에 의존하여 소프트웨어가 개발됨으로써 각 프로그래머들의 특성에 따라 시스템 분석, 개발방법론, 코딩(coding) 방법, 산출된 Document간의 불일치가 많이 발생하였으며 유지보수시 그 소프트웨어를 개발하였던 담당자가 아니면 곤란했던 한계점을 많이 내포하고 있었다. 그러나, 최근 소프트웨어 공학 기술의 눈부신 발달로 이러한 문제점들을 해결하기 위하여 정보공학 방법론에 의한 고유의 소프트웨어 개발절차 들의 정립, 표준 Document 기법 정립, Computer Aided Software Engineering(CASE) 도구 등의 도입으로 체계적인 소프트웨어의 개발과 개발기간의 단축은 물론 실질적인 품질향상과 소프트웨어 생산성 향상을 도모할 수 있게 되었다.

원전 보호계통에 장착되는 필수안전 소프트웨어의 경우 무엇보다도 소프트웨어의 안전성이 확보되어야 하며 반드시 이에 대한 검증이 뒤따라야 한다. 소프트웨어의 안전성과 검증이 강조되는 만큼 원전 필수안전 소프트웨어를 개발할 때 이에 적합한 개발 방법론을 설정함은 물론이고 이를 뒷받침 해 줄 수 있는 적절한 CASE 도구와 이를 이용한 필수안전 소프트웨어의 자동생산이 필요하다. 본 논문에서는 원전 필수안전 소프트웨어의 자동생산 패러다임을 실증하기 위하여 월성 2/3/4 호기 증기발생기 수위로 인한 원자로 정지의 로직을 그 실험모델로 설정하여 분석 및 설계를 Activity Chart 및 Statechart로 모델링하고 그래픽 패널을 설계한 다음 Statemate MAGNUM toolset을 이용하여 K&R C 코드를 자동으로 생산하는 과정을 실증한다.

II. 원전 필수안전 소프트웨어의 자동생성

2.1 증기발생기 수위로 인한 원자로 트립의 요구사양명세서 분석

증기발생기 수위로 인한 원자로 트립 신호는 첫째, 증기발생기수위측정을 통한 트립탐지 둘째, 원자로출력에 따른 트립조건에 따라 좌우된다.

ㅇ 트립이 탐지되고 원자로출력이 Log Power 이상일 때 True 값이 된다.

ㅇ 그렇치 않을 경우는 False 값이 된다.

[트립탐지]

(1) 3개의 증기발생기 수위 센서중 어느 하나라도 high 설정치(setpoint) 값 보다 크거나 같으면 트립탐지 값은 True가 된다.

(2) 3개의 증기발생기 수위 센서중 어느 하나라도 low 설정치(setpoint) 값 보다 작거나 같으면 트립탐지 값은 True가 된다.

(3) 그렇치 않으면 트립탐지 값은 False가 된다.

[트립 조건]

(1) 만약 Average flux power 및 Ion chamber logarithm power가 각각 설정치(setpoint) 값 이하라면 트립탐지는 disable 된다.

(2) 만약 Average flux power 또는 Ion chamber logarithm power가 각각 설정치(setpoint) 값 보다 크거나 같다면 트립탐지는 enable 된다.

(3) 그렇치 않으면 트립 조건은 변하지 않은 상태로 남는다.

2.2. 환경 모델링(Environmental Modeling)

환경 모델링이란 분석 대상에 대한 총괄도표(context diagram)를 activity chart로 생성하는 것이다. 즉, 분석 대상인 증기발생기 수위로 인한 원자로 트립 파라메타의 분석범위, 입출력장치 및 목표시스템이 가져야 할 성능 및 제약조건을 activity chart로 도식화 한 것이다. 본 논문에서 분석범위는 월성 원전 2/3/4호기의 7가지의 원자로 트립 파라메타중 하나인 증기발생기 수위로 인한 원자로 정지를 대상으로 하였다. 입력은 센서로 부터 값이 들어온다. 출력은 모니터 화면에 디스플레이되는데 센서 하나가 설정치 값(setpoint)을 넘었을 경우 채널트립(channel trip)이 디스플레이되면서 트립 신호가 나가며 채널 트립(D,E,F 채널)이 2개 이상 발생하였을 경우 트립(actual trip) 이라는 디스플레이와 함께 원자로 트립신호가 나간다. 원자로의 트립은 D,E,F 채널의 2/3 로직에 따라 하위의 설정치값을 초과하였을 경우는 바로 원자로 트립이 발생하게 되며 상위의 설정치값을 초과하였을 경우는 터빈이 정지되면서 곧바로 원자로 정지로 이어진다. 따라서 출력장치는 패널 화면으로 정의할 수 있다.

제약조건은 원자로를 안전하게 정지시켜야 하므로 반드시 실시간으로 수행되어야 한다. 환경 모델링의 과정을 요약하면 다음과 같다.

첫째, 총괄도표(context diagram)를 작성한다. 둘째, 분석대상의 명칭을 부여하고 주변환경인 입출력장치들을 정의한다. 셋째, 정의한 입출력장치인 terminitor에 대하여 input, output, body 부분을 기술한다.

환경 모델링상에서의 기능은 크게 정상모드(normal mode)와 트립모드(trip mode)로 분할되게 되는데 이 기능은 다시 각각 4개의 기능으로 나누어진다. 정상모드와 트립모드는 각각 condition control(COND_CNTL) 이라는 control activity의 제어(control) 하에 있게 된다.

여기서 control activity는 logpower, LSP(Low Set Point), HSP(High Set Point)와 신호 D1,D2,D3,D4, E1,E2,E3,E4, F1,F2,F3,F4의 값을 가지고 현재 입력으로 받은 신호값이 정상범위 또는 경보범위 모드에 있는지 트립범위에 있는지 아니면 logpower 모드에 있는지를 결정하게 된다. 정상모드는 Low Alarm, 정상, Hi Alarm을 구분하여 모니터에 디스플레이 하게 된다.

입력신호가 트립 범위에 들어오게 되면 트립모드는 다시 판단(decision)이라는 control activity에 의해 channel trip 인지 actual trip인지를 판별하게 된다. (그림 1)

2.3. 행위 모델링(Behavioral Modeling)

행위모델링(Behavioral Modeling)은 총괄도표(context diagram)의 다음단계로써 activity

chart 또는 statechart를 이용하여 하위 단계의 기능을 분석하게 된다. 하위단계에서는 기능을 표현하는 activity나 control을 표현하는 activity를 statechart로 표현할 수 있다. 또한, 구조적 계층이 하위수준으로 더 내려갈 경우 activity chart 형식의 계속적 분할이 가능하다. COND_CNTL 을 예로들면 센서로 부터 읽은 값이 high 또는 low 설정치(setpoint) 값을 넘었을 경우 channel trip 모드가 작동하도록 control 해 주며 그렇치 않고 센서로 부터 읽은 값이 정상범위 또는 경보범위에 있을 경우는 normal_mode 가 작동되도록 제어 한다. (그림 2)

그림 2의 control activity의 behavioral 모델링과정을 요약하면 다음과 같다.

첫째, 모든 control activity는 statechart 또는 P-spec(process specification) 형태로 표현할 수 있다. 둘째, 상위 activity(부모 activity)와 하위 activity(자식 activity)는 상호 조화(match)를 이루어야 한다. 즉, 계층구조적인 관계를 유지하면서 부모 activity가 가지고 있는 input 및 output을 상속 받는다. 셋째, 모든 data-flow에 대하여 primitive level까지 event, condition, data-item, information flow 등의 자료사전(data dictionary entry)을 정의한다.

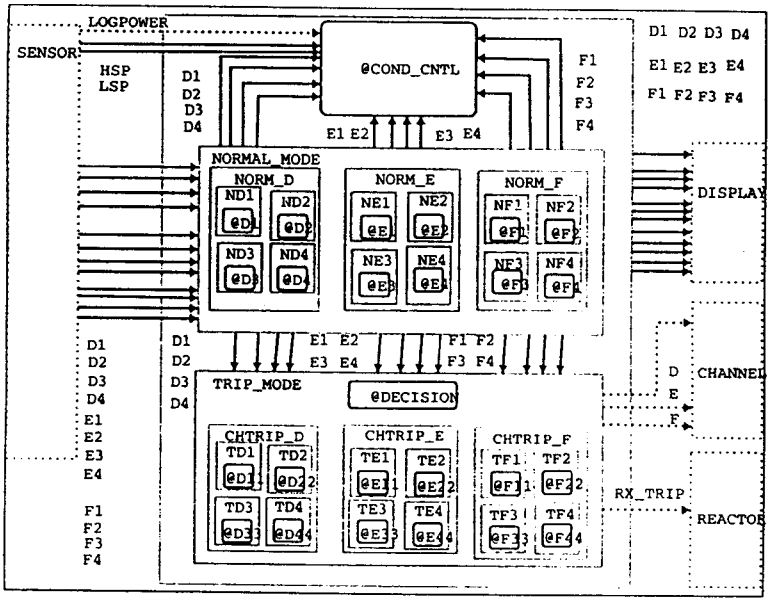

그림 1. 총괄도표(context diagram) 모델링

2.3.1 NORM_D 행위 모델링(behavioral modeling)

NORM_D의 기능은 COND_CNTL 하에서 D1,D2,D3,D4의 입력신호가 정상 범위내에 있을 경우에 작동하는 기능이다. D1,D2,D3,D4의 입력신호가 정상이면 볼트로 입력된 신호를 엔지니어링 값인 퍼센트로 환산한다. D1,D2,D3,D4의 입력신호가 Lo 경보 범위내에 있으면 볼트로 입력된 신호값을 퍼센트로 변환함과 동시에 Lo 경보 이벤트(event)를 발생시킨다. 마찬가지로 D1,D2,D3,D4의 입력신호가 Hi 경보 범위내에 있으면 Hi 경보 이벤트(event)를 발생시킨다. NORM_E, NORM_F의 경우도 마찬가지이다.

2.3.2 CHTRIP_D 행위 모델링(behavioral modeling)

CHTRIP_D 기능은 COND_CNTL 하에서 D1,D2,D3,D4의 입력신호가 트립 범위내에 있을 경우에 작동하는 기능이다. D1,D2,D3,D4 입력신호가 Hi로 인한 트립이면 볼트로 입력된 신호를 엔지니어링 값인 퍼센트로 환산한 다음 Hi channel trip을 시킨다. 또한, D1,D2,D3,D4 입력신호가 Lo 트립 범위내에 있으면 Lo channel trip 이벤트를 발생시킨다. CHTRIP_E, CHTRIP_F의 경우도 마찬가지 이다.

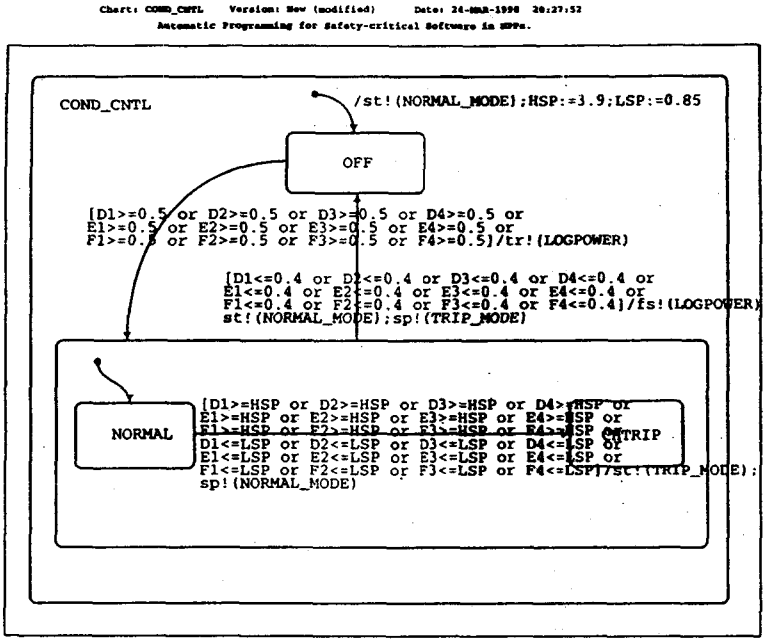

그림 2. 행위(behavioral) 모델링

2.3.3 decision control activity의 behavioral modeling

decision control activity는 현재 발생된 channel trip이 하나이면 channel trip 상태를 그대로 유지하고 하나 이상이면 2 out of 3 logic을 적용하여 실제로 원자로를 정지 시킨다. 이때 두 개 이상의 Hi channel trip으로 인한 트립일 경우 터빈을 먼저 정지시키고 난 다음 원자로를 정지시킨다. 그렇치 않고 Lo channel trip 일 경우 곧바로 원자로를 정지시킨다. (그림 3)

2.4. 그래픽 패널 설계

그래픽 패널은 그래픽 사용자 인터페이스에 해당된다. 각각의 센서로 부터 받은 입력 신호를 디스플레이 한다. 입력 신호에 따른 Lo 및 Hi 경보를 띄어주고 Lo 및 Hi channel 의 트립 상태를 디스플레이 한다. D,E,F 채널 트립은 2 out of 3 logic에 따라 Hi channel에 의한 트립이면 터빈 및 원자로의 정지를 Actual Trip 창에 표시해 주고 Lo channel에 의한 트립이면 곧 바로 원자로 정지를 Actual Trip창에 띄워준다(그림 4). 그래픽 패널이 완성되면 앞서 모델링한 context diagram의 모델링과 behavioral 모델링 부분을 그래픽 패널 부분과 바인딩 시켜고 속성(attribute)을 정의하여 시뮬레이션을 통해 모델을 검증(verification)하고 확인(validation) 한다.

2.5. Module chart design

분석 단계에서 모델링한 각각의 기능들을 소프트웨어 공학 원리인 boss rule, transform rule, transaction rule 등을 적용하여 각각을 모듈에 top-down 형식으로 할당한다. 트립 파라메타의 경우 일반적으로 안전성 문제 때문에 모두가 상호 독립적으로 구성되도록 되어 있다. 따라서 본 논문에서 예로든 월성 원전 2/3/4 호기 증기발생기 수위로 인한 트립의 경우 총 7개의 트립 파라

메타중 하나로써 하나의 기능이 하나의 모듈로 일대일 대응된다. 하나의 기능이 하나의 모듈로

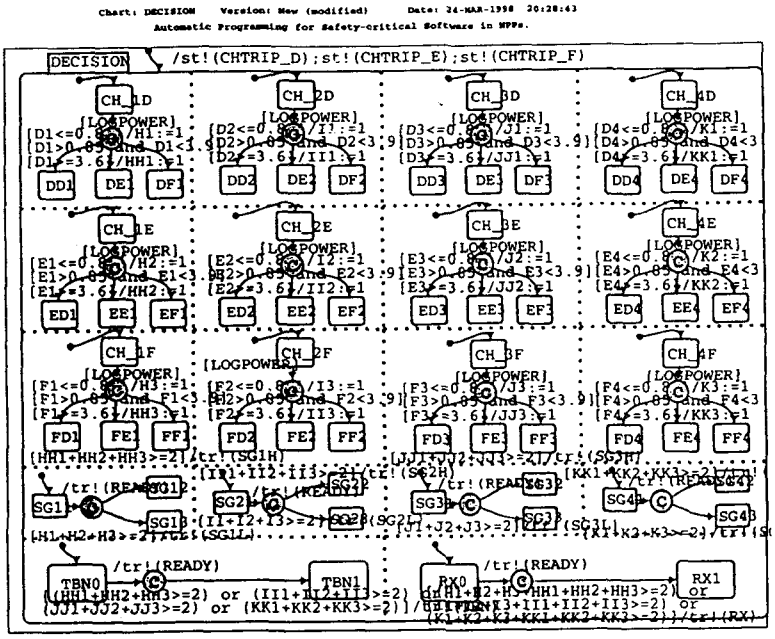

그림 3. 2/3 decision logic 모델링

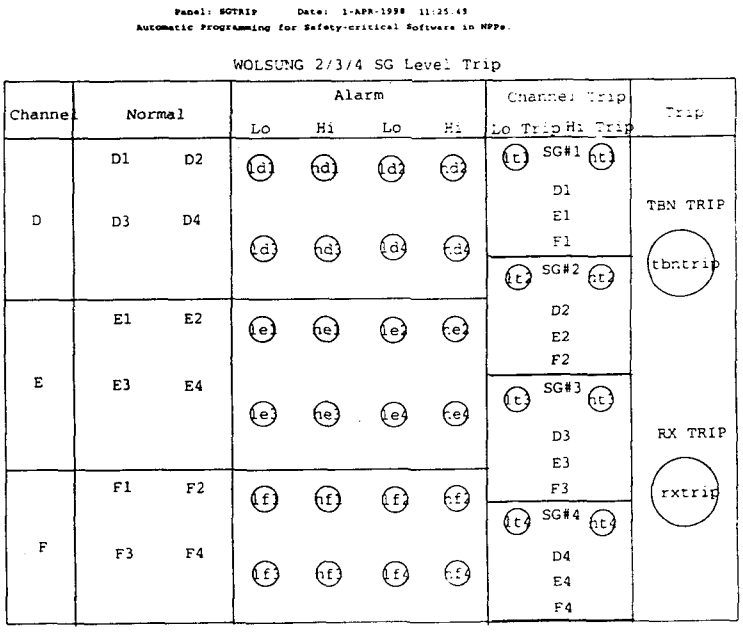

그림 4. 그래픽 패널 설계

할당될 경우는 특별한 경우로써 모듈 차트를 작성하지 않아도 된다. 이는 코드 자동생성을 위한 과정에서 요구사양명세를 분석한 모델링을 설계모듈에 일대일로 할당하여 모듈화하면 되기 때문이다. 이러한 경우는 특수한 경우로써 내상 소프트웨어의 복잡도(complexity)가 낮고 단순할 경

우이다. 복잡도가 낮아 일대일로 기능 대 모듈이 1:1로 할당될 경우 분석과 설계를 동시에 할 수 있는 경우가 되는데 이경우가 바로 여기에 해당된다. 그렇치 않은 경우(M : 1 또는 M : N)는 반드시 기능할당 과정을 통하여 모듈챠트를 작성하여야 한다.

2.6. 코드 자동생성 및 실행

분석과 설계가 완성되면 Statematemate MAGNUM toolset의 일부인 Sharpshooter/C 코드 생성기를 이용하여 K&R C 코드를 자동으로 생성한다(그림 5). K&R C 코드를 자동으로 생성하기전 인터페이스에 필요한 외부 프로그램이 있을 경우 즉, test bench 프로그램, 통신 프로그램 또는 Data Acquisition 프로그램 등을 삽입하여 코드를 자동으로 생성할 수 있다. 코드 생성기를 통하여 K&R C 코드가 자동으로 생성되면 컴파일 및 링크 과정을 통하여 실행화일을 만들 수 있다. 최종 결과물인 소스코드와 실행코드는 기계 독립적으로서 다른 기계에 이식할 수 있으며 수정 및 재컴파일이 가능하다. 소스코드에 대한 약간의 수정이 요구될 때 처음의 모델링과정을 거쳐 K&R C 코드의 자동생산하는 과정을 다시 반복하는 것이 아니라 소스코드 그 자체를 일상적인 디버거(debugger) 과정을 통하여 수정하고 재컴파일하면 된다.

```
  sg32_module_init();
  dbg_init();
  pge_setup();
}

void lo_main()
{
  sg32_module_exec_all();
}

void pr_initialize()
{
  init_model_context(&model_context);
  lo_init();
  user_init();
  sched_disable();
  update();
  sched_enable();
  pge_start_graphics();
  call_cbks(TRUE);
  pge_end_graphics();
}

boolean  pr_make_step()
{
  boolean step_has_changes = FALSE;
  incr_stepN();
  sched_disable();
  lo_main();
  step_has_changes = update();
  garbage_collect() ;
  sched_enable() ;
  scheduler();
  if (!step_has_changes && (!deb_was_update()))
    return TRUE;
  pge_start_graphics();
  call_cbks(FALSE);
  pge_end_graphics();
  return FALSE;
}
```

그림 5. 자동으로 생성된 K&R C 코드의 예

III. 결 론

본 논문은 Dr. David Harel이 제안한 Statechart based Formalism과 Statemate MAGNUM toolset을 이용하여 월성 원전 2/3/4호기 증기발생기 수위로 인한 트립 로직을 모델링하고 K&R C 코드를 자동으로 생산하였다. 자동으로 생산된 K&R C 코드는 검증 및 확인이 가능하고 품질이 우수하며 적은 인력과 노력으로 소프트웨어의 생산성을 높일 수 있었다. 또한 표준 K&R C 코드이기 때문에 기계독립적이며 이식성이 우수하다는 것을 확인할 수 있었다.

IV. 참고문헌

[1] STATEMATE MAGNUM *Reference Manual*, i-Logix, 1997.

[2] STATEMATE MAGNUM *Trailblazer Reference Manual*, i-Logix, 1997.

[3] *Modeling Reactive Systems with Statechart Approach*, DAVID HAREL AND MICHAL POLITI, 1997