정형기법을 이용한 KNICS 디지털 원자로보호계통 소프트웨어 요구사항명세 개발

*김창회, *손한성, *한재복, **유준범,

* 한국원자력연구소 계측제어・인간공학연구부
** 한국과학기술원 전자전산학과 전산학전공

요 약

원전의 안전계통은 발전소가 비정상상태일 때 원자로를 보호하고, 관련 기기를 작동시켜 사고를 완화시키는 기능을 담당한다. 따라서, 디지털 안전계통에 사용되는 소프트웨어는 안전필수 소프트웨어로 분류되며 충분한 수준의 안전성을 보장하기 위해 여러가지 기법들을 적용하여 개발하고 있다. 특히, 소프트웨어 요구사항 개발에 정형명세 기법을 적용하면 요구사항들을 보다 명확하고 완전하게 명세할 수 있어 안전성을 크게 향상시킬 수 있다. 본 논문에서는 KNICS 원자로보호계통 소프트웨어의 요구사항을 정형명세하면서 얻은 경험과 장점들을 소개한다.

1. 서 론

최근 원전의 안전계통은 기존에 사용되고 있던 아날로그 시스템 대신 소프트웨어 기반의 디지털 시스템을 사용하고 있다. 국내에서도 울진 5&6호기 원자로보호계통과 공학적안전설비계통에 안전등급 PLC를 사용한 디지털 안전계통을 적용하였고, 신고리 1&2 호기 등 울진 5&6 호기 이후에 건설되는 모든 원전에서도 디지털 안전계통을 적용하고 있다.

안전계통에 사용되는 응용 소프트웨어는 안전성을 중요시하는 안전성 필수 소프트웨어(safety critical software)이며, 이 소프트웨어는 개발의 초기단계인 요구사항 명세 단계에서부터 정형기법(formal method)을 도입함으로써 안전성을 더욱 향상시킬 수 있다.

정형기법(formal method)은 복잡한 소프트웨어 시스템이 지니는 제반 문제들을 해결하기 위해 제안된 기법으로서 크게 정형명세(formal specification)와 정형검증(formal verification)으로 구분된다[1]. 정형명세는 소프트웨어 개발 초기단계에서 개발자가 모든 요구 사항들을 생략하지 않고 명확하게 명세하도록 유도함으로써 소프트웨어의 안전성을 크게 향상시킬 수 있는 기법으로 인정 받고 있다. 특히, 개발하려는 시스템의 특성에 알맞은 특화된 정형명세 기법들이 많이 제시되고 있고, 개발 초기 단계에서 보다 명확하게 모든 요구 사항들을 명세 하려는 노력이 여러 분야에서 꾸준히 진행되고 있다[2]. 정형검증 기법은

이러한 정형명세를 기반으로 하여 모델체킹(model checking)[3]이나 정리증명(theorem proving)[4] 등의 검증을 통해서 정형명세된 소프트웨어의 안전성을 증명하는 기법이다.

캐나다의 AECL은 Darlington 발전소 안전계통 개발에 확장된 SCR[5]을 사용해서 소프트웨어 요구사항을 정형명세하였다. 이 기법은 먼저, 보다 명확하게 요구사항을 명세하기 위해서 SCR이 지니는 세 종류의 테이블을 한 종류의 테이블 SDT(Structured Decision Table)로 통합했다. 또한, DFD의 일종인 FOD(Function Overview Diagram)를 사용하여 전반적인 자료의 흐름을 볼 수 있도록 했으며, 시간제약(timing constraints) 조건을 명세하기 위해서 섬세한 시간 함수들(timing functions)을 제공하고 있다. 이것은 원자력 발전소 안전계통에 적용된 최초의 정형명세 기법이며, 또한 한국 월성 2~4호기 안전계통인 SDS2에도 이 기법이 적용되었다[6].

현재 시운전 중인 울진 5&6호기 DPPS(Digital Plant Protection System)는 소프트웨어 요구사항을 슈도 코드(pseudo code) 즉, 특정 조건일 동안 어떤 행위가 수행되어야 한다는 while-then 형태의 논리로 요구사항을 명세하였다[7]. 그러나 이 방법은 정형명세 기법이 아닌 자연어 표현을 좀 더 논리적으로 표현한 것이다.

한편, KNICS 사업에서는 기존에 제시된 AECL의 SCR 방법을 수정, 보완한 NuSCR을 개발하였다[8]. NuSCR은 SCR과 마찬가지로 Parnas' Four-Variable Model[9]에 기초하며, 이 모델에서 정의되는 relations를 보다 명확하게 명세하기 위해서 세 가지의 추가적인 변수 모델을 사용한다. 이것은 function variable, history variable, timed-history variable로서 각각 SDT(Structured Decision Table), FSM(Finite State Machine), TTS(Timed Transition System)를 이용해서 표현된다. 이러한 요소들을 포함하고 있는 NuSCR의 원활한 사용을 위해서 명세 지원 도구인 NuEditor가 개발되었으며, 이 도구를 사용하여 요구사항을 명세한다.

본 논문은 원전 안전계통의 응용소프트웨어를 명세 하는데 적합하도록 개발된 정형명세 기법인 NuSCR을 이용해서 KNICS 원자로보호계통 소프트웨어 요구사항명세 개발과정과 정형명세 개발을 통해 얻은 경험들을 소개하고 있다.

2. KNICS 원자로보호계통

KNICS 원자로보호계통은 4개의 채널로 구성되며, 각 채널의 구성은 그림 1과 같으며 비교논리프로세서 (BP), 동시논리프로세서 (CP), 자동시험 및 연계프로세서 (ATIP), 운전원모듈로 구성된다. 이들 프로세서들은 KNICS 사업을 통해 개발되는 안전등급 PLC를 사용한다. 비교논리프로세서와 동시논리 프로세서는 안전성 필수 소프트웨어 요건을 만족해야 하며, 자동시험 및 연계프로세서와 캐비닛운전원모듈은 안전성 관련 소프트웨어요건을 만족한다.

비교논리프로세서는 노심보호연산기 및 공정계측계통으로부터 트립변수를 취득하고, 이 값과 트립설정치를 서로 비교하여 트립 또는 예비트립 상태를 결정한다. 각 채널에는 동일

한 구성을 갖는 2개의 비교논리프로세서(그룹 1 및 2)가 설치된다. 그룹 1 및 2 비교논리프로세서는 동일한 트립논리를 가지며, 서로 독립적으로 논리를 수행한다. 비교논리프로세서는 발전소 기동 및 정지시 불필요한 트립을 발생시키지 않기 위해 운전우회(operating bypass) 신호를 취득한다. 비교논리프로세서에서 발생된 트립상태신호는 동일 채널 및 타 채널의 동시논리 프로세서로 전송되며, 동시논리 프로세서는 각 채널의 비교논리 프로세서에서 전송된 트립상태신호를 조합하여 2/4 보팅논리를 계산한다. 비교논리 프로세서의 트립상태신호는 안전데이터링크(SDL)를 통해 동시논리 프로세서로 전송된다. 비교논리 프로세서는 비교논리 작동의 건전성과 안전데이터링크의 건전성을 감시하기 위해 박동신호를 발생시켜 각 채널의 동시논리 프로세서로 전송한다.

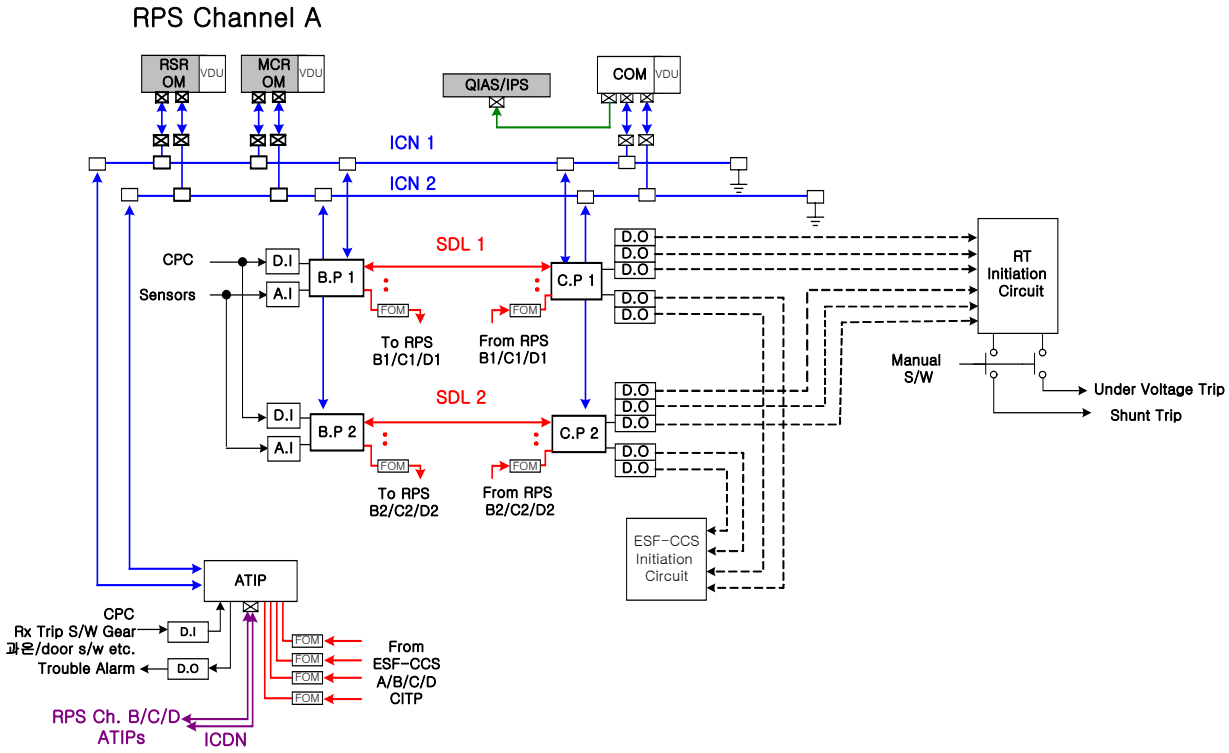


그림 1 원자로보호계통 한 채널의 구성

동시논리프로세서는 각 채널의 비교논리 프로세서에서 전송된 트립상태신호를 조합하여 2/4 보팅논리를 수행한다. 2/4 보팅논리는 각 변수 별로 수행되며, 보팅결과를 조합하여 원자로 트립 및/또는 공학적안전설비-기기제어계통 작동 개시신호를 발생시킨다. 각 채널에는 동일한 구성을 갖는 2개의 동시논리프로세서(그룹 1 및 2)가 설치된다(그림 1 참조). 각 동시논리프로세서는 동일 그룹의 비교논리프로세서로부터 트립상태신호를 제공 받아 2/4 보팅논리를 수행한다. 원자로 트립 및 공학적안전설비-기기제어계통 작동 개시신호는 디지털 출력모듈을 통해 원자로트립 개시회로 및 공학적안전설비-기기제어계통 개시회로로 전송된다. 동시논리프로세서는 각 채널의 비교논리 프로세서에서 전송된 박동신호의 건전성을 감

시하여 어떤 채널에 오류가 있을 경우 그 채널의 비교논리프로세서 출력은 모두 트립상태로 간주한다. 동시논리프로세서는 유지보수를 위한 트립채널우회(trip channel bypass) 및 전 채널우회(all bypass) 신호를 디지털 입력모듈을 통해 취득한다.

자동시험 및 연계프로세서는 원자로보호계통 각 채널의 운전상태를 감시하고, 수동개시자동시험을 수행한다. 자동시험 및 연계프로세서는 비교논리 및 동시논리프로세서의 건전성을 감시하고, 노심보호연산기계통, 원자로 정지차단기, 캐비닛 내부 전원공급장치 및 온도, 캐비닛 문의 개방신호 등 채널 내 기기들의 작동상태를 감시한다. 자동시험 및 연계 프로세서는 타 채널의 운전상태를 취득하고, 공학적안전설비-기기제어계통의 운전상태를 감시한다. 수동개시자동시험은 운전원 또는 보수요원의 요구에 따라 수행된다. 시험은 캐비닛운전원모듈을 통해 개시되고, 자동시험 및 연계프로세서에서 관련된 시험신호를 발생시킨다.

3. 원자로보호계통 정형기법 요구사항명세 개발

3.1 NuSCR

요구사항명세 개발에 정형기법을 적용함으로써 얻을 수 있는 가장 큰 이점은 개발자로 하여금 개발하고 있는 시스템에 대해 명확하게 요구사항을 명세하도록 유도해 준다는 것이다. 이는 모든 정형명세 기법이 지니는 공통적인 특징으로 다음과 같은 장점을 제공한다.

- 모든 입력과 출력을 명확하게 규정할 수 있다.
- 개발자가 의도하는 구체적인 수행 논리들을 명확하게 기술할 수 있다.
- 시스템이 지니고 있는 내부적인 가정들 즉, 일반적으로 인식되므로 생략되던 것 들을 모두 명확하게 기술하게끔 유도함으로써 명세를 보다 완전(complete)하게 기술할 수 있다.

본 논문에서는 NuSCR을 이용하여 작성한 원자로보호계통 비교논리프로세서 요구사항명세에 대해 기술한다.

NuSCR은 기존에 제시된 AECL의 SCR에 기반 하는 방법론을 수정, 보완하여 원자력 발전소의 제어 시스템 소프트웨어를 명세 하는데 보다 유용하게 사용될 수 있도록 개발된 정형명세 기법으로 보다 명확하게 명세하기 위해 SCR에 비해 function variable, history variable, timed-history variable과 같은 추가적인 3가지 변수 모델을 사용한다. 이들 변수 모델들은 각각 SDT(Structured Decision Table), FSM(Finite State Machine), TTS(Timed Transition System)를 이용해서 표현된다. 각각의 세 변수 모델들은 서로 다른 행위를 명세하는데 유용하게끔 특징지어져 있다. Function variable은 수학적인 함수 관계를 표현하는데 사용되며 SDT와 같은 테이블을 사용한다. History variable은 수학적인 함수 보다는 상태(state)를 중심으로 명세할 때 보다 쉽게 명세 되는 내용을 표현할 때 사용된다. History

variable은 오토마타의 일종인 FSM으로 표현된다. 또한, Timed-history variable은 시간제약 조건이 추가된 내용을 명세할 때 사용되며, 시간 개념이 추가된 오토마타의 일종인 TTS를 사용한다. 이와 같이 서로 다른 특성을 지니는 변수들 간의 relationship은 DFD의 일종인 FOD에 의해서 표현된다. 각각의 변수들은 FOD 상에서 하나의 독립된 노드(node)로서 표현되며, 각 노드들은 입력과 출력을 갖는다. 또한 FOD는 계층적으로 표현된다. 이와 같은 여러 요소들을 포함하고 있는 NuSCR의 원활한 사용을 위해서 명세 지원 도구인 NuEditor가 개발되어 사용되고 있다.

NuSCR은 다음과 같은 고유한 특징을 지니고 있다.

- 대부분의 정형명세 기법들은 수학적인 기호나 특수한 의미의 diagram을 사용하므로 일반적인 엔지니어가 사용하기에 쉽지 않다. 그러나 NuSCR은 현장 엔지니어들에게 친숙한 테이블과 흐름도 만을 사용하기 때문에 현장의 개발자들이 쉽게 이해하고 사용할 수 있다.
- NuSCR은 원자력 발전소에서 사용하는 제어용 소프트웨어를 명세하기에 쉽도록 정의되어 있다. 즉, 명세하려는 내용의 특성에 따라 3 종류 - SDT(Structured Decision Table), FSM(Finite State Machine), TTS(Timed Transition System)로 분류하여 명세하도록 함으로써 보다 쉽고 간결(compact)한 명세가 가능하다.
- NuSCR은 지원 도구인 NuEditor를 통해서 입력/출력에 대한 기본적인 완전성/일관성을 보장해 주고 있으며, XML 출력을 이용한 자동 검증도구와의 연계 또한 쉽게 할 수 있다.

3.2 비교논리프로세서 정형기법 요구사항명세

비교논리프로세서는 모두 18개 신호를 주기적으로 입력 받아 관련 트립논리를 통해 트립 및 예비트립 상태신호를 발생시킨다. 이들 18개 트립논리를 설정치 종류별로 그룹핑하면, 고정설정치 트립, 수동리셋형 가변설정치 트립, 자동비율제한형 가변설정치 트립, 디지털 트립으로 나눌 수 있다. 이들 논리에 대해 작성된 정형명세는 기본적으로 다음과 같은 구성을 갖는다.

- 트립논리의 요건
- 트립논리의 입력변수
- 트립논리의 상수
- 트립논리의 출력변수
- 가정 및 고려사항
- State Transition Diagram
- NuSCR을 이용한 트립논리 요구사항명세

본 논문에서는 고정설정치 하강트립논리에 대해 작성된 요구사항명세를 예시로 제시한다. 고정설정치 하강트립논리를 사용하는 증기발생기-1 저수위 트립논리(*th_SG1_LVL_RPS_Lo_TRIP*)에 대한 요구사항을 간단하게 기술하면 다음과 같다.

Requirement for *th_SG1_LVL_RPS_Lo_TRIP*

① 공정 변수 값이 미리 결정된 설정치 보다 감소할 경우에 트립 신호를 발생한다.
② 트립 상태가 되면 트립 설정치는 정해진 히스테리시스 만큼 증가하고, 트립 상태가 해제되면 처음의 트립 설정치를 다시 유지한다.
③ 채널 에러, 모듈 에러, 입력값 에러 등이 발생하면 설정치가 히스테리시스 만큼 변경되지 않고 트립상태 신호를 발생한다.

Input Variables

① f_X : 공정변수
② f_Module_Error : 모듈 오류를 전달하는 변수 (error = 1)
③ f_Channel_Error : 채널 오류를 전달하는 변수 (error = 1)
④ f_X_Valid : 공정변수의 valid 여부를 전달하는 변수 (invalid = 1)

Constants

① k_X_Trip_Setpoint : 공정변수 X의 trip set-point
② k_Trip_Delay : trip임을 판정하는데 요구되는 time delay
③ k_X_Trip_Hys : 공정변수 X의 trip hysterisis
④ k_X_Trip_Setpoint : 공정변수 X의 trip set-point

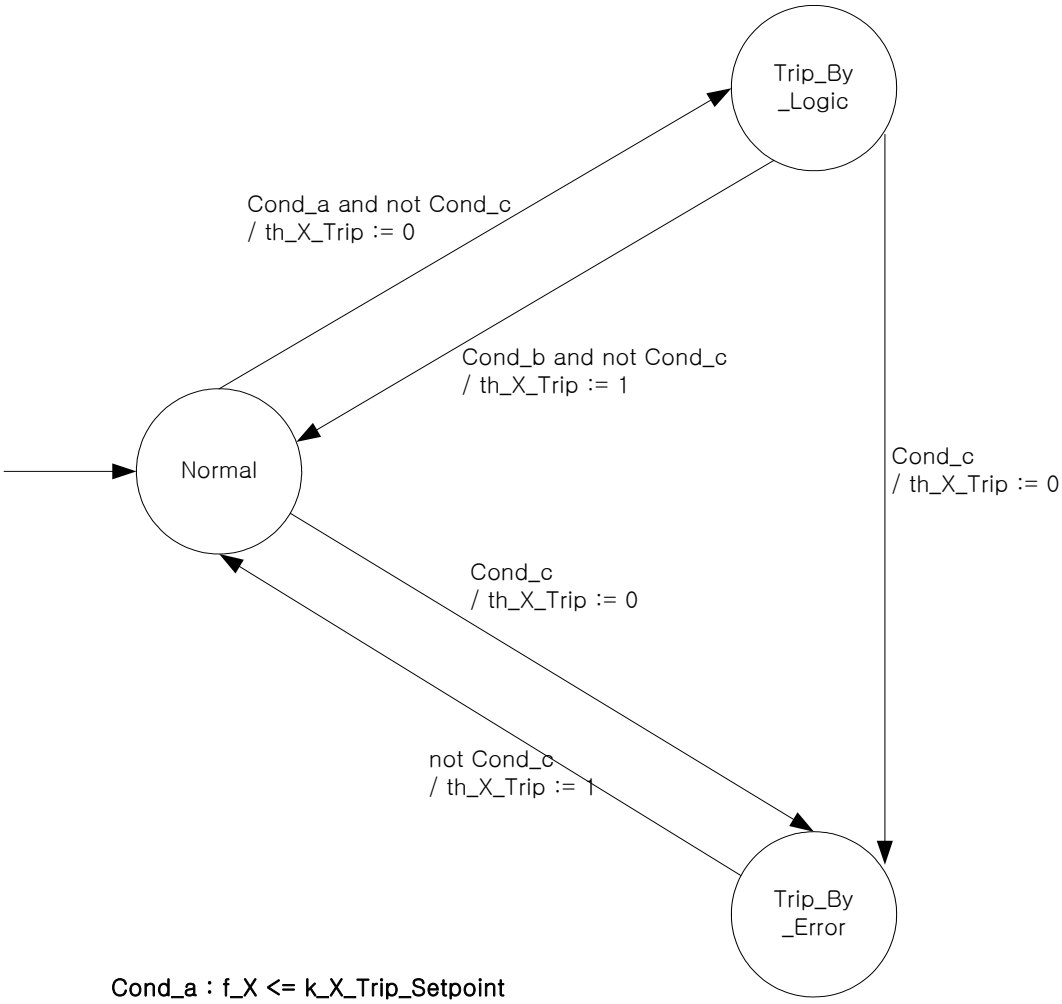
Output Timed History Variable

① th_X_Trip : 공정변수의 트립 (trip = 0)

Assumptions and Considerations

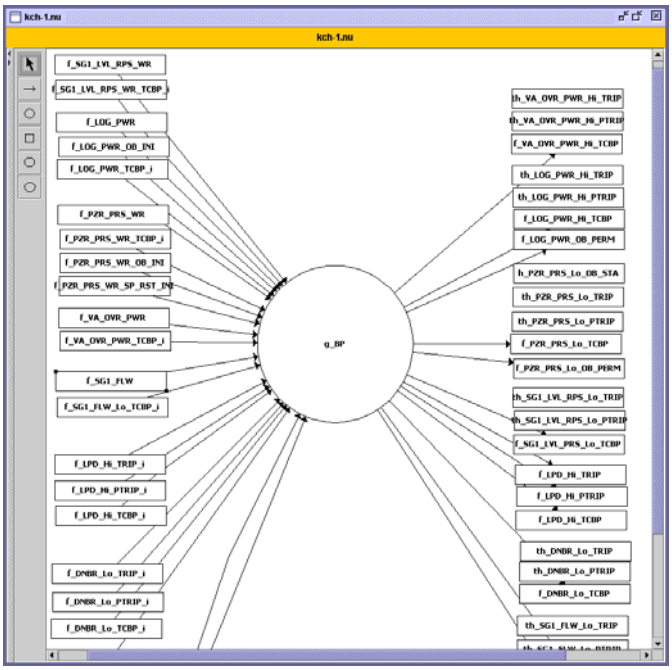
① 정상적인 trip logic에 의해서 trip이 발생한 경우에는 hysterisis를 적용해서 설정치를 재조절 해야 한다.
② 그 외의 경우 즉, channel error, module error, value error인 경우에는 초기 상태에서 처음부터 다시 시작한다고 가정한다

Trip Decision State Transition Diagram



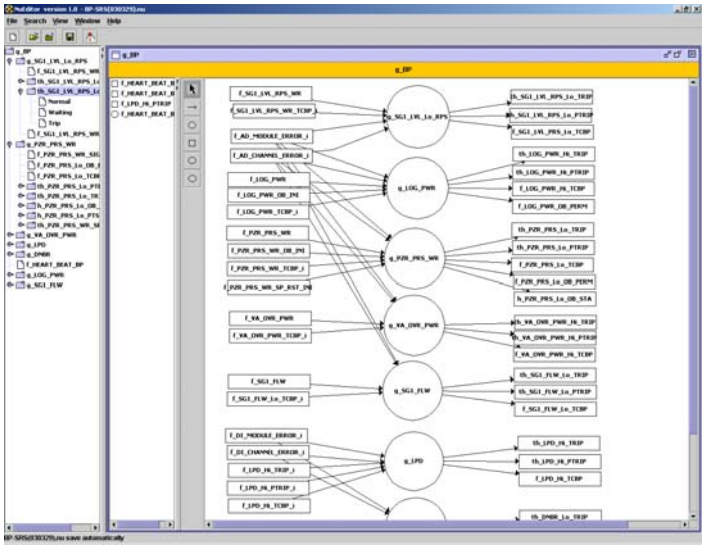
위에서 정의된 th_X_Trip의 내용을 살펴보면 다음과 같다. 초기 상태는 Normal이며, 공정값이 트립 설정치 보다 작게 되면 Trip 상태로 전이한다. Normal 상태에서 채널 에러나 모듈 에러, 공정값의 에러 등 외부 에러가 발생하면 바로 Trip 상태(th_X_Trip = 0)로 전이한다. 일단 트립이 발생한 후에는 모든 외부 에러들이 정상이고, 공정값이 원래의 트립 설정값에서 히스테리시스 값을 더한 값 보다 상승할 경우에만 정상상태(th_X_Trip=1) 바뀌면서 Normal 상태로 복귀하게 된다.

NuSCR Specification for BP (최 상위의 FOD인 *g_BP*)



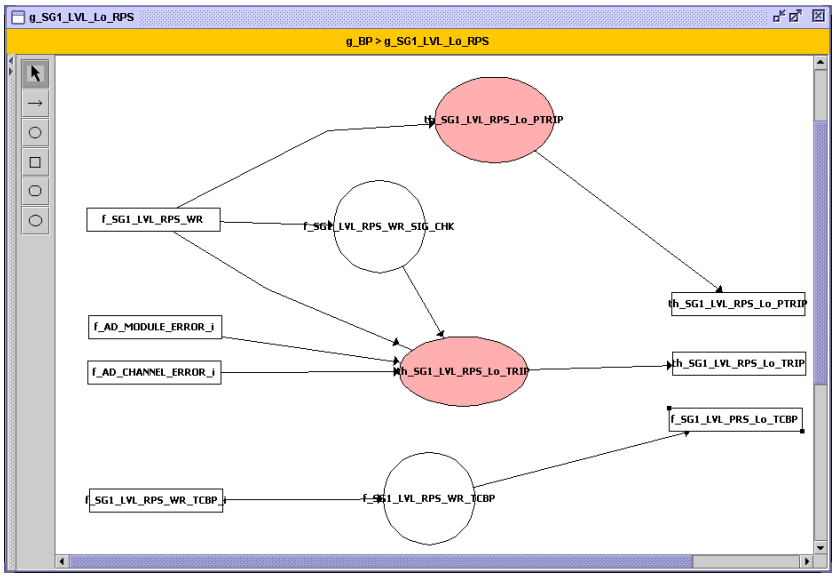
위의 그림은 NuEditor로 작성한 NuSCR 명세의 일부로서, 가장 상위의 FOD인 *g_BP*를 표현하고 있다. 노드 *g_BP*의 왼쪽에 있는 노드들은 BP로의 입력을 의미하며, 오른쪽에 있는 노드들은 BP로부터 계산되어 발생되는 출력들을 의미한다.

NuSCR Specification for BP (한 단계 하위의 FOD인 *g_BP*)



위 그림은 NuEditor로 작성한 NuSCR 명세의 일부로서, 최상위 노드인 *g_BP*에 대한 한 단계의 하위 명세를 수행한 결과에 대한 NuEditor 화면이다. NuSCR 지원 도구인 NuEditor의 좌측 부분은 FOD의 계층구조를 표현하고 있으며, 오른쪽에는 편집 화면이 위치한다. 앞에서 언급한 BP의 특성에서 유추할 수 있듯이 "g_"로 표현된 각 노드들은 모두 각각의 입력 변수에 대한 트립 논리를 대표하고 있으며, 이들간에는 interaction이 없음을 알 수 있다. 이러한 독립적인 특성은 각 트립 논리 부분을 모듈화 시킬 수 있으며, 이는 후에 각 논리가 주어진 자연어 명세대로 정확하게 동작하는 가를 증명하기 위해서 정형검증 기법을 적용할 때에도 유용하게 사용될 수 있다.

NuSCR Specification for g_SG1_LVL_Lo_RPS



위의 그림은 NuEditor로 작성한 NuSCR 명세의 일부로서, g_SG1_LVL_Lo_RPS 대한 NuSCR 명세를 나타낸다. 위의 그림에서 원으로 표현된 function variable 노드인 f_SG1_LVL_RPS_WR_SIG_CHK는 표 1 에 정의되어 있으며, 타원으로 표현된 timed history variable 노드인 th_SG1_LVL_RPS_Lo_TRIP은 그림 2에 정의되어 있다.

표 1 SDT for f_X_Valid

Conditions		
k_X_MIN <= f_X <= k_X_MAX	T	F
Actions		
f_X_Valid := 0	X	
f_X_Valid := 1		X

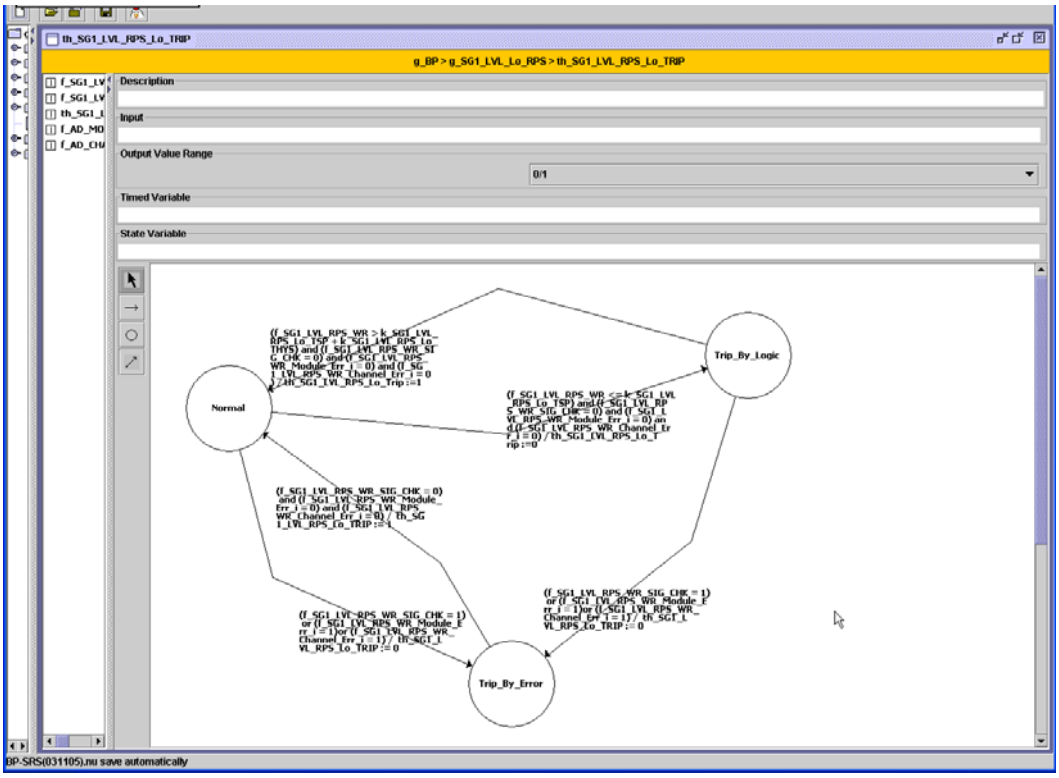


그림 1 Timed history variable node인 th_SG1_LVL_RPS_Lo_TRIP NuSCR 명세

이러한 일련의 과정을 통해 요구사항명세를 작성하면서 논리적인 오류뿐만 아니라 숨겨진 가정들을 보다 명확하게 드러냄으로써 보다 완전한 소프트웨어 요구사항 명세를 작성할 수 있었다. 이러한 경험을 통해 정형명세 기법인 NuSCR이 원자력 발전소 안전계통뿐만 아니라 제어계통 응용 소프트웨어를 명세하는데 유용하게 사용될 수 있음을 확인할 수 있었고, NuSCR이 정형명세 기법으로서의 장점 외에도, 원자력 분야의 소프트웨어를 명세하는데 적합하게 개발된 기법이라는 점을 실증할 수 있었다.

4. 결 론

본 논문에서는 원전 안전계통의 응용소프트웨어를 명세 하는데 적합하도록 개발된 정형명세 기법인 NuSCR을 이용해서 KNICS 원자로보호계통 소프트웨어 요구사항명세 개발과정과 정형명세 개발을 통해 얻은 경험들을 소개하였다. NuSCR은 원자력 분야에 종사하는 엔지니어들에게 익숙한 notation을 채택함으로써, 현장의 개발자들이 큰 무리 없이 약간의 교육만 받으면 바로 사용할 수 있다는 장점을 지니고 있다. 또한, NuSCR은 정형명세 도구인 NuEditor를 사용하여 보다 체계적으로 명세할 수 있게끔 지원하며, 입력/출력간의 기본적인 완전성/일관성 문제도 도구 상에서 충족시켜 줄 수 있음을 확인하였다. NuEditor를 통해서 작성된 NuSCR 명세는 XML 포맷의 데이터로 변환되기 때문에 이를 이용하면 정형검증이 가능할 것으로 판단된다.

NuSCR을 이용해서 요구사항명세를 정형기법으로 작성함으로써 원자로보호계통에 대한 이해를 증가시킬 수 있었고, 자연어로 작성된 명서의 오류나 생략되기 쉬운 가정들, 그리고 생각으로만 있던 구체적인 수행논리들을 명확하게 드러냄으로써 명확하고 완전한 소프트웨어 요구 명세를 작성할 수 있었다.

참고문헌

[1] Doron A. Peled, *SOFTWARE RELIABILITY METHODS*. Springer, 2001.

[2] Edmund M. Clarke and Jeannette M. Wing, Formal Methods: State of the Art and Future Directions. *ACM Computing Survey*, 1996.

[3] E. A. Emerson, Edmund M. Clarke and A. P. Sistla. Automatic verification of finite-state concurrent system using temporal logic specification. *ACM Trans. Programming Languages and Systems*, 8(2):244-263, 1986.

[4] D. vam Dalem. *Logic and Structure*. Springer-Verlag, 3 edition, 1994

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

[6] Wolsong NPP 2&3&4. Software requirements specification for shutdown system 2 PDC. 86-68350-SRS-001, June 1993.

[7] Ulchin NPP 5&6. Digital Plant Protection System Software requirements specification for the Ulchin NPP 5&6.

[8] NuSCR TR

[9] D. Parnas and J. Madey. Functional documentation for computer systems engineering. CRL 237, Telecommunications Research Institute of Ontario(TRIO), McMaster Univ., Hamilton, Ontario, 1991.

[10] Junbeom Yoo, Sungdeok Cha, Changhui Kim, Younju Oh, Formal Requirements specification for digital reactor protection systems, *Journal of KISS submitted*, 2003.

[11] KNICS-RPS-SRS101 Rev.01, 원자로보호계통 소프트웨어요구사항명세서, 2003.