PtolemyII를 이용한 디지털 원자력 발전소 보호시스템의 통합 설계

[0]김진현*, 황혜정*, 이나영**, 최진영*
*고려대학교 컴퓨터학과
**서울대학교 원자력공학과
e-mail : *{jhkim,hjhwnag,choi}@formal.kroea.ac.kr, **grasia2@hotmail.com

Co-design of Nuclear Power Digital Plant Protection System using Ptolemy

Jin Hyun Kim*, Hye Jung Hwang*, Na-Young Lee**, Jin Young Choi*
*Dept. of Computer Science, Korea University
**Dep. Of Nuclear Power, Seoul National University

요 약

원자력 발전 및 항공 시스템과 같은 실시간 시스템의 설계는 대표적인 Safety-critical 시스템으로서 그 설계로부터 구현에 이르기까지 다양한 방법으로 안정성을 보장하는 설계방법이 연구되고 있다. 특히 이러한 내장형 시스템은 근래에 들어 하드웨어-소프트웨어 통합설계를 통해 설계초기부터 안정성과 일관성 등을 높일 필요가 있다. 본 연구에서는 아날로그 및 디지털이 혼합된 Heterogeneous 시스템의 통합 설계 도구인 PtolemyII[1]을 이용하여 원자력 발전 내장형 시스템의 일종인 Digital Plant Protection 시스템을 설계하고 이를 시뮬레이션 함으로 Safety-critical 시스템 가운데 가장 높은 등급을 요하는 시스템에 통합설계를 적용시켜 본다. 그리고 이에 대한 정형 검증기법을 제안한다.

1. 서론

내장형 시스템이란 어떤 기능은 컴퓨터에 의해 수행되고 어떤 부분은 컴퓨터가 아닌 부분으로 수행되는 시스템을 말한다. 이러한 내장형 시스템은 소프트웨어의 융통성의 특징을 가지고 있고, 하드웨어의 성능을 이용한다. 원자력 발전소 보호계통 내장형 시스템은 대표적인 Safety-critical 내장형 시스템이다. 이러한 시스템은 원래 아날로그를 기반으로 한 시스템이지만 최근 들어 부품의 고갈로 인한 문제를 극복하고 시스템의 융통성을 더하기 위해 하드웨어와 소프트웨어가 함께 탑재된 내장형 시스템으로 만들려 하고 있다.

이러한 시스템의 구현은 주로 하드웨어와 소프트웨어를 각각 만들어 인터페이스를 추가하여 설치한 다음, 시험하는 형태로 만들어진다. 즉 초기 시스템 요구 명세를 가지고 하드웨어와 소프트웨어가 될 부분을 선택한 후, 이를 각각 만들고 인터페이스를 통해 전체 시스템을 만드는 식으로 설계되고 구현된다. 하지만 이렇게 개별 설계 및 구현은 많은 문제를 가지고 있다.

첫째, 하드웨어와 소프트웨어는 각각의 다른 성질을 가지고 있다. 즉 하드웨어는 그 특성상 시간적 제약을 비교적 정확히 지킬 수 있으나 소프트웨어는 그렇지 못하다. 즉 소프트웨어는 시간적으로 비 결정성을 지니고 있다. 따라서 하드웨어와 서로 시간적으로 맞지 않은 경우로 인해 시스템이 오류를 일으킬 수 있다.

둘째, 시스템에 대한 확인 검증이 수월하지 않다. 하드웨어와 소프트웨어를 각각 따로 검증하고 인터페이스를 통해 전체 검증을 실시해야 하기 때문에 전체 시스템의 검증은 어렵고 많은 시간을 소모할 수 있다.

셋째, 시스템의 전체의 설계상의 문제가 구현까지 이어질 경우, 이러한 오류의 발생은 하드웨어와 소프트에어의 설계로 다시 거슬러 올라가야 한다. 따라서 설계 및 구현까지의 프로세스를 다시 밟아가야 하는 단점을 지니고 있

다. 따라서 시스템 개발 시간이 늘어나는 단점을 가지고있다.

이러한 내장형 시스템의 구현의 문제를 해결하기 위해 하드웨어와 소프트웨어가 함께 구성되어 있는 시스템을 설계하기 위해 하나의 언어로 설계 후, 검증을 거친 후, 이를 하드웨어와 소프트웨어로 부분으로 나누어, 각각을 구현하는 통합설계가 연구되고 있다.

이러한 통합설계로는 Polis[2], Esterel[3], STATEMATE, Ptolemy 등이 있다. 본 연구에서는 특히 Ptolemy 를 safety-critical 시스템의 설계에 적용시키고 이를 검증하는 기법을 제안하고자 한다. 2 장에서는 통합설계 도구인 Ptolemy 의 특징에 대해 기술하고, 3 장에서는 대표적인 원자력 발전 보호계통인 DPPS(Digital Plant Protection System)에 대해 논하고 이에 Ptolemy 를 적용하고자 한다. 4 장에서는 Ptolemy 의 가장 큰 특징이라 할 수 있는 Heterogeneous 시스템의 통합 시뮬레이션을 통해 하드웨어와 소프트웨어의 검사를 실시하고자 한다. 5 장에서는 보다 완전한 설계를 구현하고자 이러한 설계에 정형기법을 적용시켜 검증하는 기법을 제안하고 6 장에서 결론 및 향후 연구 과제로 본 논문을 마치고자 한다.

2. PtolemyII 를 통한 통합설계

PtolemyII 는 Ptolemy 프로젝트의 일부로 개발되고있는 소프트웨어 프레임워크 이다. 자바 기반의 컴포넌트 어셈블리 프레임워크로서 Vergil 이라는 그래픽 사용자 인터페이스를 가지고 있다. Vergil 은 그 자체로 역시 PtolemyII 에 의해 정의된 컴포넌트의 모임이다.

Ptolemy 프로젝트는 동시성, 실시간 내장형 시스템의 모델링, 시뮬레이션과 설계에 대한 연구이다. 이 프로젝트의 바탕이 되는 기본 원칙은 컴포넌트들 사이의 상호작용을 제어하는 잘 정의된 계산모델(models of computation)을 사용하는 것이다. 이러한 것의 문제점은 heterogeneous 한 혼합된 계산모델을 사용한다는 것이다.

PtolemyII 는 확장되고 있는 도메인들로 이루어져 있다. 각각의 도메인은 계산모델을 구현한 것이다. 또한 PtolemyII 는 컴포넌트 라이브러리를 포함하고 있으며 대부분의 컴포넌트는 domain polymorphic 하여 다양한 도메인에서 수행할 수 있다. 대부분은 또한 data polymorphic 하여 다양한 데이터 타입에서 수행된다. 이러한 도메인은 아래와 같다.

- CT: continuous-time modeling,
- DE: discrete-event modeling,
- FSM: finite state machines,
- PN: process networks,
- SDF: synchronous dataflow
- CSP: communicating sequential processes, (shipped only in the full release)
- DDE: distributed discrete events (experimental - full release only),
- DT: discrete time, (experimental - full release only),
- Giotto: periodic time-driven (experimental - full release only) and
- GR: 3-D graphics (experimental - full release only).

본 연구에서는 이러한 다양한 도메인을 통해 아날로그 시스템 및 디지털 시스템을 다양하게 모델링 할 수 있다.

본 논문에서는 이러한 특성들을 이용하여 아날로그 신호와 디지털 신호가 동시에 입력으로 받아들이는 DPPS 를 모델링하여 시뮬레이션 하고자 한다. 또한 이러한 것을 어떻게 정형기법을 이용하여 검증할 수 있는지를 제시하고자 한다.

우선 다음 절에서는 본 논문에서 설계하고자 하는 DPPS 에 대해 논한다.

3. Digital Plant Protection System 의 설계

<그림-1>에서 보는 것처럼 하나의 신호를 네 개의 같은 채널을 통해 검사하는 Diversity 한 시스템이다. 본 연구에서 가정하는 DPPS 는 기본적인 성질은 동일하지만 불필요한 몇 가지 특성을 제외한다.

본 논문의 DPSS 시스템은 크게 A,B,C,D 4 개의 각각의 독립적인 equipment room 들로 구성되어 있으며, 이 각각의 equipment room 들은 크게 bistable processor, coincidence processor , RT, ESF 로 구성되어 있다. 이 각각의 모듈의 자세한 동작 사항은 다음과 같다.

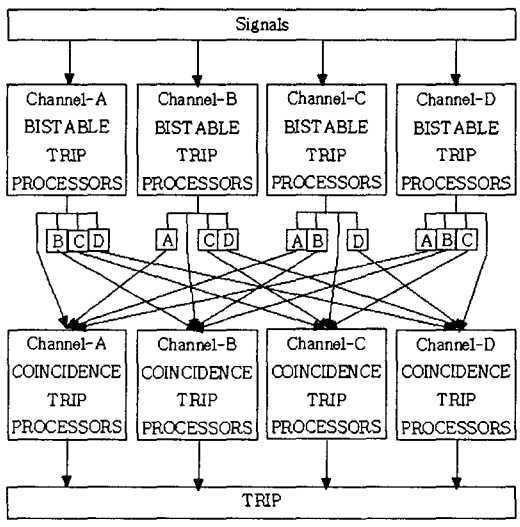

그림 1. Digital Plant Protection System

1) bistable processor

각각의 4 개의 채널에서 모니터링 하는데 필요한 프로세스의 개별적인 측정값을 받아들인다. bistable function 은 측정한 프로세스를 미리 정해진 제한 값과 비교하여 trip 상태로 전이할 것인지를 결정한다. 원자로가 start-up 되고 shutdown 될 동안 불필요한 trip 을 발생시킬 수 있는 제한 값을 갖는 bistable function 은 불필요한 trip 을 막는 operating bypass 에 의해 처리되게 된다. Operating bypass 는 프로세스가 정해진 값의 범주 내에 있으면, 작동자에 의해 수동적으로 동작하지만 프로세스가 정해진 값의 범주를 벗어나면, 자동적으로 제거되게 된다.

2) coincidence processor

각각의 채널에서 coincidence processor 는 bistable function 마다 local coincidence logic(LCL) 알고리즘을 적용한다. LCL 알고리즘은 각각 4 개의 A, B, C, D 채널에서 생기는 출력을 입력 받아 세 개 이상이 error 상태에 있는지를 voting 해서 그래도 error 상태에 있으면 위험한 상태를 알리기 위해 trip 하게 된다. 즉 다시 말해서, local coincidence logic 은 다음과 같은 입력을 받는 coincidence signal 을 생성하게 된다. {AB, AC, AD, BC, CD, ABC, ACD, BCD, ABCD}

3) RT, ESF

4 개의 독립된 채널 중 3 개 이상의 신호가 4 회 이상 지속될 경우, 제어봉으로 연결된 전원을 차단하여 중력에 의한 제어봉의 자유 낙하에 의해 핵반응을 제어할 수 있도록 하는 RT(Reactor Trip), ESF(Engineered Safety Features)

DPPS 가 만족해야 하는 중요한 성질은다음과 같다.

Property : Safety_01

Always (((*ERROR i* ∧*ERROR i*∧*ERROR*$_i$)→

(*ERROR i* ∧*ERROR i*∧*ERROR*$_k$)→

(*ERROR i* ∧*ERROR i*∧*ERROR*$_k$)→

(*ERROR i* ∧*ERROR i*∧*ERROR*$_k$)→*TRIP*)

(*i*≠ *j*≠ *k* 0≤ *i,j,k*≤ 3))

Property Safety_01 은 만약 3 개 이상의 채널에서 에러가 검출된다면 그 즉시 trip 신호가 발생해야 함을 요구조건으로 둔 것이다

다음 절에서는 PtolemyII 를 이용하여 DPPS 를 모델링한 결과와 시뮬레이션 결과를 보여줄 것이다.

3.1. Ptolemy 를 이용한 Digital Plant Protection System 의 설계명세

<그림-2>는 PtolemyII 로 명세한 DPPS 시스템이다. 이 시스템은 아날로그 신호 하나와 디지털 신호 하나를 각각 4 채널씩 입력 받게 된다. 만약 신호에 문제가 있다면 이

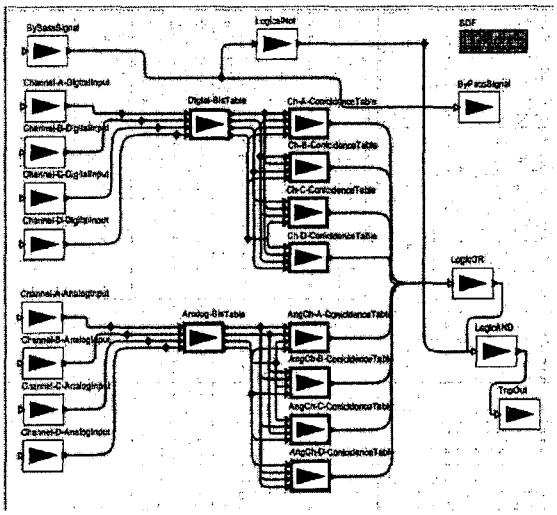

그림 2. PtolemyII 를 이용한 4 채널 DPPS

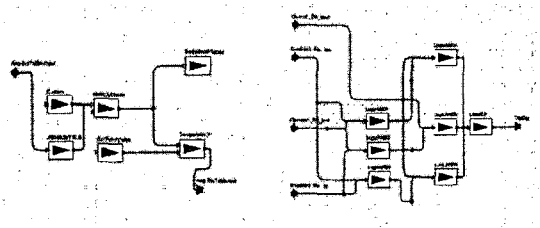

그림 3. 좌: 아날로그 Bistable, 우: Coincidence Table

를 Coincidence Table 로 내려보내게 되고 Coincidence Table 에서 다른 3 개의 채널에서 같은 신호를 입력 받아 voting 을 하되 자신의 채널 외 두 개 이상의 신호가 오류를 감지할 경우, Trip 신호를 발생해서 제어봉을 떨어뜨리는 시스템이다. <그림-2>의 맨 위의 BiPassSignal 은 시스템의 오픈 시, 개방되는 신호로서, 특정한 시간이 지난 후, 비로서 시스템의 오류를 감지하게 하는 역할을 한다. 예를 들어, 특정 온도가 올라 간 다음, 그 온도 이하를 오류를 발생시켜야 할 경우라면, 특정 온도까지 올라 가야만 오류 감지 기능이 수행되어야 하기 때문이다.

<그림-2>의 상위 4 개의 신호는 디지털 신호로써 0/1 의 신호를 받아 1 은 정상적인 신호, 0 은 오류 감지 신호를 구별하게 된다. 만약 0 의 신호가 감지 될 경우, Coincidence table 의 기능을 수행하게 된다. 하위 4 개의 채널은 아날로그 신호를 받아들이게 되는데 본 논문에서는 임으로 setpoint 를 120 으로 정해 이를 넘어가는 것을 오류로 감지하게 된다.

그림 4 의 좌측은 아날로그의 bistable 이다.

이 모델링은 Synchronous Data Flow 도메인에서 모델링한 것으로 주로 데이터의 흐름으로 시스템의 행위를 묘사하게 된다. 즉 하나의 데이터가 변함에 따라 전체 시스템의 부

분의 데이터가 변화됨을 보여줌으로 시스템의 행위를 묘사하게 되는 것이다. Synchronous dataflow 도메인은 stream 의 계산의 regular computations 을 다룬다. Dataflow 모델은 시그널 프로세싱에서, 프로세스 네트워크의 특별한 경우이다. Dataflow 모델은 일련의 atomic firing actor 로서 프로세스 네트워크 프로세스를 구성하게 된다. Synchronous dataflow 는 deadlock 이나 boundedness 가 결정적인 유용한 성질을 가진 특별한 제한된 경우이다.

다음 장에서는 이 시스템의 모델을 검사하기 위해 PtolemyII 의 가장 큰 장점이라 할 수 있는 Heterogeneous 시스템의 시뮬레이션의 결과와 특성을 보이겠다.

4. PtolemyII 를 이용한 통합 시뮬레이션

PtolemyII 는 앞에서 언급한 것처럼 Heterogeneous 한 모델의 시뮬레이션 기능을 제공한다. 본 논문에서는 이를 응용하여 아날로그 시스템과 디지털 시스템을 모두 하나로 통합 설계하여 시뮬레이션 한다. <그림-4>에서는 아날로그 신호들이 변화를 볼 수 있다. 본 논문의 DPPS 의 시뮬레이션에서는 일련의 아날로그 입력에 대해 단위시간 별로 측정하게 된다. <그림-4>에서 볼 수 있는 것처럼 setpoint 인 120 이상을 넘어가는 3 채널의 채널이 있을 때는 Trip 신호가 발생한다.

이 외에도 디지털 신호로서 1/0 값을 측정하여 3 채널 이상에서 0 이 나오면 Trip 신호를 발생한다. <그림-4>의 TripOutDisplay 창에서는 아날로그 및 디지털 신호 채널에서 Trip 신호를 발생시키는 모든 경우에 Trip 을 발생한다.

이 실험을 통해 아날로그 및 디지털 신호가 통합된 시스템의 시뮬레이션이 쉽게 가능함을 알았고, 또한 원자력 발전 내장형 시스템에 이를 적용시킴으로 설계의 효용성을 증대시켰다.

5. PtolemyII 의 설계를 위한 정형검증

원자력 발전 내장형 보고계통시스템은 일반적으로 Safety-critical 시스템으로 분류되어 다양한 방법으로 확인 검증되어 그 안전성이 증명되어야 한다. 따라서 근래 들어 이러한 설계에 정형기법을 적용하여 그 안전성을 높이려는 연구가 진행되고 있다.

PtolemyII 는 잘 정의된 계산모델을 지니고 있으며 이들은 대부분 정형명세 언어로 바뀔 수 있는 특징을 지니고 있다.

따라서 본 논문에서는 다음과 같은 방법으로 PtolemyII 의 모델을 검증할 것을 제안한다.

특정 도메인의 시간적인 개념에 맞는 정형명세 언어를 선택하여 각 컴포넌트와 동일한 행동을 하는 정형명세언어로 기술된 컴포넌트를 구현한다. 이렇게 구현된 정형명세 언어로 기술된 컴포넌트를 이용하여 PtolemyII 로 모델링된 시스템과 동일한 정형명세 언어로 구현된 시스템이 존재하게 된다. 이는 정형검증을 통해 검증할 수 있게 된다.

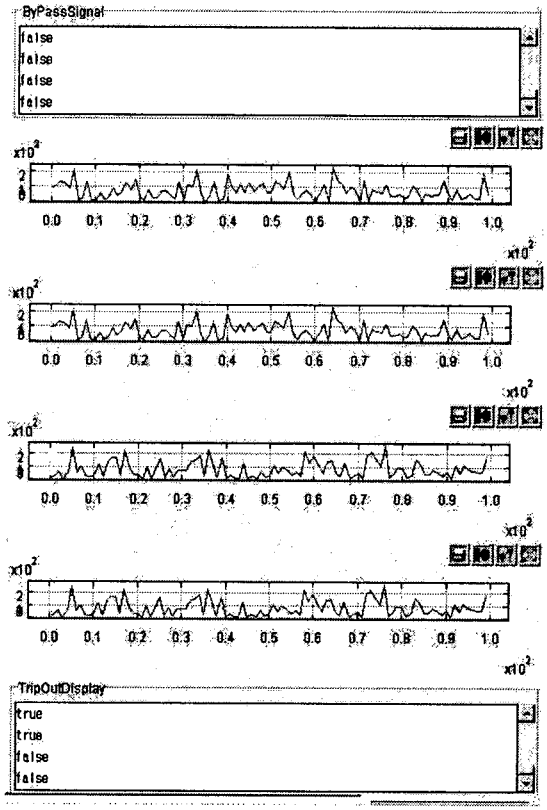

그림 4. PtolemyII 로 시뮬레이션 된 DPPS

이러한 검증을 통해 시스템의 다양한 특성을 확인 검증할 수 있게 되어 보다 안전한 시스템을 구현하게 된다.

6. 결론 및 향후 연구 과제

본 논문에서는 Safety-critical 시스템의 일종인 원자력 발전 내장형 보호계통 시스템을 통합설계하기 위해 PtolemyII 를 이용하여 설계하고 이를 검증하는 기법을 제안하였다. 특히 본 연구를 통해 Heterogeneous 시스템 설계도구인 PtolemyII 의 편리성과 다형성, 정형검증을 통한 시스템의 안정성 확보에 주안으로 두고 있다.

향후 연구 과제로는 PtolemyII 의 정형명세 언어로의 전환과 이를 구현하여 실제 적용시키는 연구가 진행될 것이다.

7. 참고문헌

[1] Edward A.Lee, John Davis II, et.al, Heterogeneous Concurrent Modeling and Design in Java, User Manual, U.C .Berkeley, 2001,March 15,

[2] http://www-cad.eecs.berkeley.edu/Respep/Research/hsc/abstract.html

[3] http://www.esterel.org