NuSTPA : 발전소보호계통을 위한 STPA 기반의 안전성 분석 도구

김민우[1], 이동아[1], 유준범[1], 이장수[2]
[1]건국대학교 컴퓨터공학부, [2]한국원자력연구원

NuSTPA : A STPA-based safety analysis tool for PPS

Minwoo Kim[1], Dong-Ah Lee[1], Junbeom Yoo[1], Jang-Soo Lee[2]
[1]Konkuk University, Division of Computer Science and Engineering, [2]Korea Atomic Energy Research Institute

Abstract - 대표적인 안전필수시스템(Safety critical system) 중 하나인 원자력 발전소는 충분한 수준의 안전성을 확보하기 위해 다양한 안전성 분석 기법이 적용되어 왔다. 원자력 시스템의 규모가 커지고 복잡해지면서 기존의 기법을 사용한 원자력 시스템의 안전성 분석이 한계점을 나타내고 있다. STPA (System Theoretic Process Analysis)는 시스템 이론을 기반으로 시스템의 안전성을 분석하는 기법으로서, 소프트웨어와 하드웨어뿐만 아니라 사람, 기관, 환경 요소와 같이 시스템의 개발과 운영에 관련된 요소들을 하나의 모델로 표현하여 위험을 분석하는 기법이다. STPA는 다양한 분야의 안전성 분석을 위해 사용되어 왔으나 분석에 필요한 비용이 많이 들고 기법을 지원하는 도구에 대한 연구가 부족해 분석의 어려움을 겪고 있다. 원자력 분야의 안전성 분석과 관련된 위와 같은 어려움을 해결하고자 발전소보호계통(Plant Protection System)의 안전성 분석을 위해 STPA를 활용한 안전성 분석 기법을 수행할 수 있는 도구인 NuSTPA를 개발하였다. NuSTPA는 사고의 인과 관계 모델을 control structure로 표현하여 Diagram을 작성할 수 있으며, 정형기법을 기반으로 하는 발전소보호계통 소프트웨어 명세 언어인 NuSCR을 참조해 안전성 분석을 수행할 수 있다. NuSTPA를 통해 STPA를 보다 쉽게 활용하여 안전성 분석을 수행할 수 있으며, 자동화된 일부 절차는 STPA 분석 비용을 절감시킨다. 사례연구로서 KNICS (Korea Nuclear Instrumentation and Control System) 프로젝트에서 개발된 RPS (Reactor Protection System)를 대상으로 NuSTPA를 활용한 안전성 분석을 수행하였다.

1. 서 론

원자력 발전소의 디지털 계측제어시스템(I&C : Instrumentation and Control)은 안전필수시스템(Safety critical system)으로서 사고 발생 시 막대한 피해를 초래할 수 있다. 이러한 시스템의 안전성 확보를 위하여 FTA (Fault Tree Analysis)[1], FMAE(Failure Mode and Effect Analysis)[2], HAZOP (HAZard and OPerability analysis)[3]과 같은 다양한 안전성 분석 기법이 적용되어 왔다. 위와 같은 기법들은 수십 년 전에 개발되어 여러 분야의 안전성 분석을 위한 기법으로 사용되고 있다. 하지만 시스템의 규모가 커지고 복잡도가 증가하면서 기존 안전성분석 기법의 한계점이 드러나고 있다. 특히 다양한 시스템이 결합되어 하나의 거대한 시스템을 이루는 현대 시스템은 기존의 안전성 분석 기법이 대상으로 했던 시스템과 규모와 복잡도 측면에서 큰 차이를 보이기 때문에 적용이 쉽지 않다. 이러한 기존 기법들의 한계를 보완하고자 제시된 STPA (System-Theoretic Process Analysis) [4] 기법은 System Theory를 기반으로 하는 시스템 모델을 대상으로 안전성 분석을 수행하는 기법이다.

STPA는 상호 작용하는 여러 개체나 시스템들을 하나의 시스템 분석 대상으로 보고, 이 시스템의 상호작용에서 위험 상황을 만드는 원인을 밝혀내는 안전성 기법으로서 다양한 분야에 적용하고 연구되고 있다. 시스템의 구성 요들을 Control Structure를 표현하고, 시스템에서 발생할 수 있는 사고에 대한 원인을 구성 요소간의 제어에 초점을 맞춰 분석하는 기법이다. STAP를 활용한 안전성 분석은 많은 시간과 높은 비용이 요구되며, 더욱이 이를 지원하는 도구에 대한 연구가 많지 않기 때문에 STPA 기법을 적용하는 것에는 어려움이 따른다.

본 논문은 STPA 기법을 원자력 발전소의 발전소보호계통(PPS : Plant Protection System)에 적용하기 위한 자동화 도구인 NuSTPA를 소개한다. NuSCR [5]은 원자력 발전소의 발전소보호계통의 소프트웨어 요구사항 명세를 위한 정형명세언어이다. NuSTPA는 NuSCR 명세를 사용하여 STPA 분석에 사용될 Control Structure의 일부를 구성하고, STPA를 사용한 안전성 분석을 수행하기 위해 개발된 도구이다. 정형명세언어를 사용한 Control Structure 구성은 STPA 절차의 일부 단계를 자동화 할 수 있도록 지원한다. 일부 절차가 자동화된 STPA 기법은 원자력 발전소 시스템의 안전성 분석에 요구되는 시간과 비용을 줄여준다. 본 논문에서 소개한 NuSTPA의 사용성을 평가하기 위하여 KNICS (Korea Nuclear Instrumentation and Control System) 프로젝트에서 개발된 RPS (Reactor Protection System)를 대상으로 SPTA 분석을 수행하였으며, STPA의 일부 절차가 자동화 될 수 있음을 확인하였다.

2. 배 경 지 식

2.1 NuSCR

NuSCR은 안전필수시스템인 원자력 발전소 디지털 계측제어시스템의 소프트웨어 요구사항을 작성하기 위해 개발된 정형명세 언어이다. SCR (Software Cost Reduction)의 확장언어인 NuSCR은 Parnas' Four-Variable Model을 기반으로 함수 관계를 수학적 모델로 표현한다. 테이블 형태인 SDT (Structured Decision Table)와 오토마타 형태인 FSM (Finite State Machine), FSM에 시간적 제약을 추가한 TTS (Timed Transition System)를 사용해 소프트웨어 요구사항을 작성한다. <그림 1>은 2개의 SDT와 각 1개의 FSM과 TTS로 이루어진 NuSCR의 예를 나타낸다.

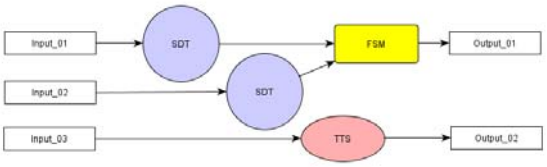

그림 1 : NuSCR FOD의 예

2.2 STAMP / STPA

STPA는 System Theory를 기반으로 하는 모델(STAMP : System-Theoretic Accident Model and Process)을 대상으로 안전성 분석을 수행할 수 있는 최신 기법이다. STAMP는 사고의 원인과 결과를 분석하는 모델로, 안전제약사항의 위반이나 부적절한 제어로 사고가 발생한다고 여긴다. 모델에서 요구하는 필수 요소는 안전제약사항(Safety constraints), 계층적 제어 구조(Hierarchical control structure), 프로세스 모델(Process model)이라는 세 가지 개념으로 이를 통해 사용하여 시스템을 표현하고 사고에 대한 시스템적인 원인을 찾는다. 모델의 구성요소는 하드웨어나 소프트웨어뿐만 아니라 운영적인 요소, 환경을 포함한 다양한 구성 요소 계층적 구조에 포함시킬 수 있다. 이러한 구성요소는 상호간에 Control과 Feedback이라는 관계로 연결되며, 전체 시스템의 안전을 위협하는 사고는 Control에 의해 발생할 수 있다고 간주한다. 특히 Control을 만들어내는 Controller는 Control을 만들어내기 위한 기준인 Process Model을 가지며, Process Model은 Controller의 행위에 관여하는 모든 정보를 포함한다. Controller와 Controller가 Control하는 대상인 Controlled Process의 관계는 <그림 2>와 같다.

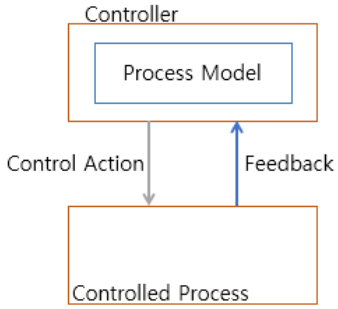

그림 2. STPA의 Controller와 Controlled Process의 관계

STPA는 위와 같은 이론에 바탕을 둔 모델의 안전성 분석을 수행하는 기법으로 4단계로 이루어져 있으며, 각 단계는 다음과 같다.

S1 : 시스템의 사고와 위험, 안전제약사항 정의
S2 : 시스템의 Control Structure 도출
S3 : STPA 1 단계 : 시스템의 위험을 유발하는 비(非)안전 제어 도출
S4 : SPTA 2 단계 : STPA 1단계의 비안전 제어의 원인을 도출

과정 중 S3에서 도출한 비안전 제어는 시스템의 위험을 일으킬 수 있는 제어이며, 이는 크게 네 가지로 나뉜다.

T1 : 제어가 제공되어야 할 경우에 제공되지 않을 경우
T2 : 제어가 제공되지 않아야 할 경우에 제어가 제공된 경우
T3 : 제어가 너무 늦거나, 이르게 혹은 잘못된 순서로 제공된 경우
T4 : 제어가 너무 길게 제공되거나, 너무 빠르게 중지된 경우

네 종류의 비안전 제어는 S4를 통해 그 발생 원인을 밝혀내게 된다. 본 논문에서 소개하는 NuSTPA는 STPA 전과정을 지원하며, 자동화 분석 기법은 Control Structure로부터 비안전 제어를 도출하는 단계인 S3를 대상으로 한다.

3. NuSTPA

3.1 NuSTP의 구조

NuSTPA는 STPA 안전성 분석 기법 수행의 과정 중 일부를 자동화 하여 기법 수행을 지원하는 도구로 Eclipse RCP (Rich Client Platform)를 기반으로 개발하였다. 도구의 전체 구조는 <그림 3>과 같다. Data Model은 STPA를 사용한 안전성 분석을 수행하기 위한 데이터를 의미하며, Safety Constraints, Accidents, Process Model과 Control Action, Feedback을 포함한 Control Structure, Unsafe Control Action을 포함한다. NuSTPA Diagram Editor는 STPA 분석을 수행하기 위한 편집기로서 NuSTPA Data Model을 Diagram으로 표현한다.

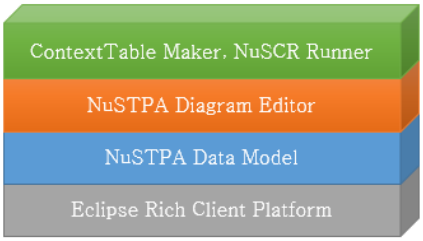

그림 3 NuSTPA 도구의 구조

NuSTPA 도구의 주요 기능은 다음과 같다.
(a) 분석에 필요한 Safety Constraint와 Accident 작성
(b) (a)에서 작성된 요소들 간의 관계를 정의
(c) Control Structure Diagram 생성 및 편집 <그림 4>
(d) Controller의 Process Model을 NuSCR로부터 자동생성
(e) NuSCR과 (d)의 결과를 통해 비안전 제어를 자동으로 생성

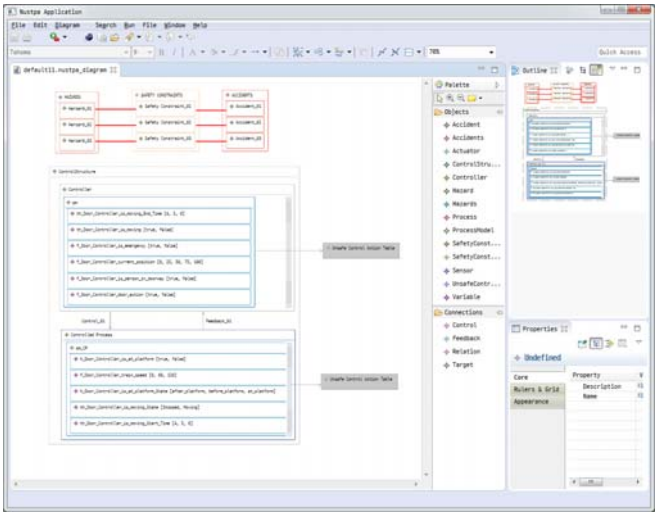

그림 4 NuSTPA Diagram Editor

3.2 ContextTable Maker & NuSCR Runer

STPA 분석을 통해 밝혀내는 비안전 제어는 Controller의 Control이 발생할 수 있는 모든 경우를 일일이 고려해 T1~4에 해당하는 모든 경우에 대응된다. 이러한 정보는 Controller의 Process Model로부터 획득하게 되는데, Process Model이 복잡해질수록 고려해야할 상황이 기하급수적으로 늘어난다. NuSTPA는 ContextTable Maker와 NuSCR Runner를 통해 S3에 해당하는 비안전 제어를 자동으로 도출한다. 특히, 원자력 발전소의 계측제어계통에 대한 위험성 분석을 위해 NuSCR로 명세된 Process Model을 사용해 비안전 제어를 도출한다 [6].

ContextTable Maker는 Controller의 Process Model을 Context Table형태로 작성하는 도구로서, NuSCR에서 사용하는 세 가지 모델인 SDT, FSM, TTS로부터 필요한 변수들을 추출하고 NuSCR에서 사용하는 모든 입력을 사용해 Context Table을 생성한다. NuSCR Runner는 Context Table과 NuSCR로 작성된 Controller의 소프트웨어 요구사항을 조합하여, Controller의 특정 Control이 발생하는 모든 경우의 수를 도출한다. 이렇게 도출된 Control과 Control이 발생하는 Context의 반대 경우를 비안전 제어로 정의하고, STPA의 나머지 단계인 S4를 수행하게 된다.

3.3 NuSTPA 적용

NuSTPA를 사용해 KNICS Project의 RPS의 안전성 분석을 수행해 보았다. S1~2를 수행하기 위해 NuSTPA Diagram Editor를 이용하였다. 시스템의 사고와 위험을 정의하고, 전체 구조를 Diagram 형태로 도출하였으며, RPS의 제어기에 해당하는 Controller의 Process Model을 NuSCR로부터 자동으로 생성하였다. S1과 S2에 해당하는 일부 결과가 <그림 4>에 나타나 있다.

자동화된 S3를 RPS의 특정 기능을 대상으로 수행한 결과는 <그림 5>와 같다. Process Model 내에 12개의 독립적인 변수를 가진 제어를 대상으로 수행한 결과 Table의 결과가 약 18억 개의 비안전 제어를 도출할 수 있었다. 현재 도출한 비안전 제어의 수준으로는 추가적인 분석이 불가능하여 S4는 진행하지 않았다.

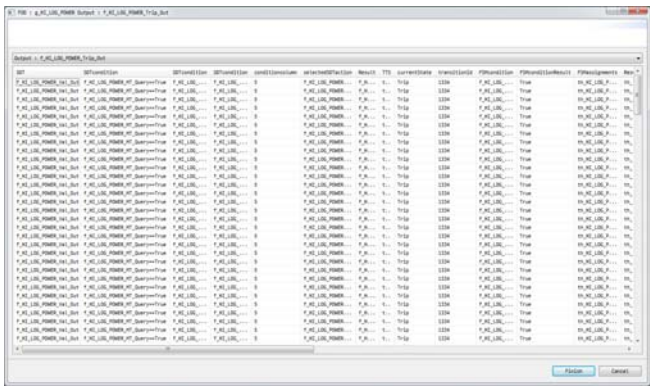

그림 5 Table 형태로 표현된 비안전 제어

4. 결 론

본 논문에서는 안전성 분석 기법인 STPA의 일부 자동화를 지원하기 위한 도구인 NuSTPA를 소개하였다. STPA의 모든 단계를 하나의 도구에서 지원하며, 분석 비용이 많이 들어가는 일부 단계를 자동화하여 비용을 줄이고자 노력하였다. 현재 자동화를 통해 도출된 결과의 양이 너무 많아 추가적인 분석을 수행하지는 않았으나, 자동화가 가능함을 확인하였다. 향후 연구로서 비안전 제어를 도출하는 개수를 줄이는 연구를 진행할 예정이다.

[참 고 문 헌]

[1] W. E. Vesely, N. H. Roberts, “Fault Tree Handbook”, Government Printing Office, 1987
[2] D. H. Stamatis, “Failure Mode and Effect Analysis: FMEA from Theory to Execution”, ASQ Quality Press, 2003
[3] http://en.wikipedia.org/wiki/Hazard_and_operability_study
[4] Nancy G. Leveson, “Engineering a Safer World: Systems Thinking Applied to Safety”, MIT Press, 2011
[5] Jumbeom Yoo, Taihyo Kim, Sumgdeok Cha, Jangsu Lee, and Han Seong Son, “A Formal Software Requirements Specification Method for Digital Nuclear Plants Protection Systems”, Journal of Systems and Software, Vol.74, No.1, pp. 73-83, 2005.
[6] Youngju Seo, “An Extended Process of STPA and Implementation of an Automatic Assistant Tool for Reactor Protection System Software”