NuSTPA : 발전소보호계통을 위한 STPA 기반의 안전성 분석 도구

김민우, 이동아, 유준범(건국대학교)
이장수(한국원자력연구원)

KU KONKUK UNIVERSITY

DEPENDABLE SOFTWARE LABORATORY

Content

- 서론
- 배경지식
  - STAMP/STPA
  - NuSCR
- NuSTPA
  - NuSTPA 구조
  - ContextTable Maker & NuSCR Runner
  - NuSTPA 적용
- 결론

서론

- 안전필수시스템(Safety Critical System)
  - 사고 발생 시 인명 피해나 심각한 환경 오염을 초래할 수 있는 중대한 시스템
    대표적인 안전필수시스템 : 원자력 발전소, 자동차, 비행기, 철도 등
  - 안전성(Safety)이 최우선으로 보장되어야 함

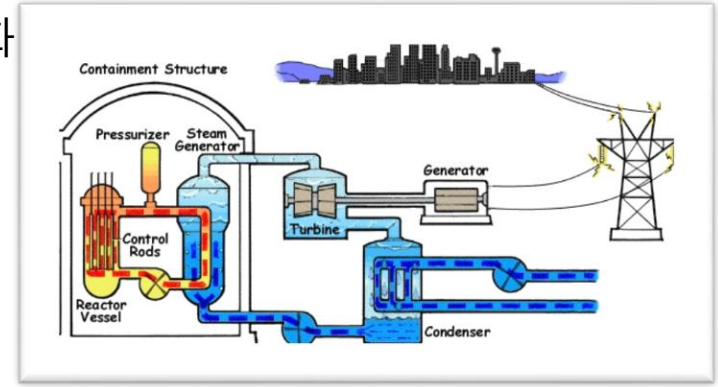
- 안전필수시스템에 적용되는 대표적인 안전성 분석 기법

  FTA (Fault Tree Analysis)

  FMAE (Failure Mode and Effect Analysis)

  HAZOP (HAZard and Operability analysis)

- 원자력 발전소의 규모가 커지고 시스템이 디지털화 됨에 따라 복잡도 증가
  - 발전소 안전성 분석의 어려움 증가



서론

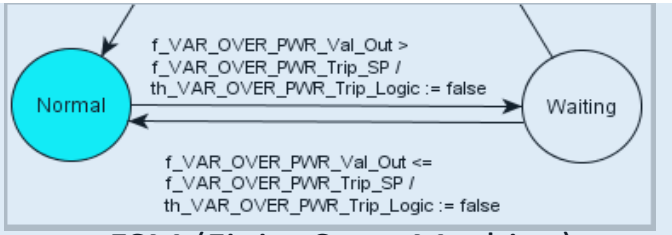
- 원자력 발전소의 규모와 복잡도가 증가함에 따라 기존 안전성 분석 적용이 어려워 짐
- STPA : 기존 안전성 분석 기법의 한계를 보완하는 새로운 안전성 분석 기법
- STPA 분석 기법을 수행하는 도구에 대한 연구가 부족하여 STPA 수행에 어려움이 따름
- NuSTPA : 원자력 발전소 디지털 I&C 시스템의 소프트웨어 요구사항 명세언어인 NuSCR을 이용한 STPA 자동화 지원도구
- KNICS Project에서 개발한 원자로 보호계통을 대상으로 Case Study 수행

배경지식 – NuSCR

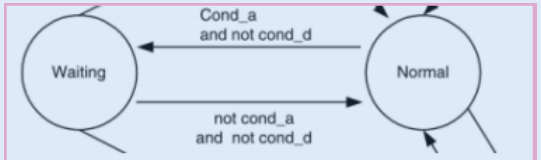
- 원자력 발전소 디지털 계측제어시스템의 소프트웨어 요구사항을 명세하도록 개발된 정형명세 언어
- 세가지 요소를 통해 시스템의 동작을 표현

Conditions	1	2
f_VAR_OVER_PWR_Trip_Status = false	T	F
Action	**1**	**2**
f_VAR_OVER_PWR_Trip_SP := h_VAR_OVER_PWR_Int_SP	O	
f_VAR_OVER_PWR_Trip_SP := f_VAR_OVER_PWR_Trip_SP_t0		O

SDT (Structured Decision Table)



FSM (Finite State Machine)



Cond_a : f_X >= k_X_Trip_Setpoint
Cond_b : [k_Trip_Delay, k_Trip_Delay]
(f_X >= k_X_Trip_Setpoint
and h_X_OB_Sta = 0)

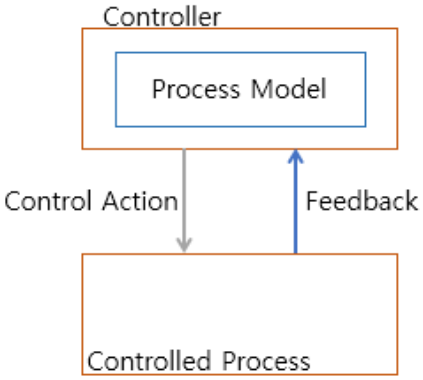
TTS (Timed Transition System)

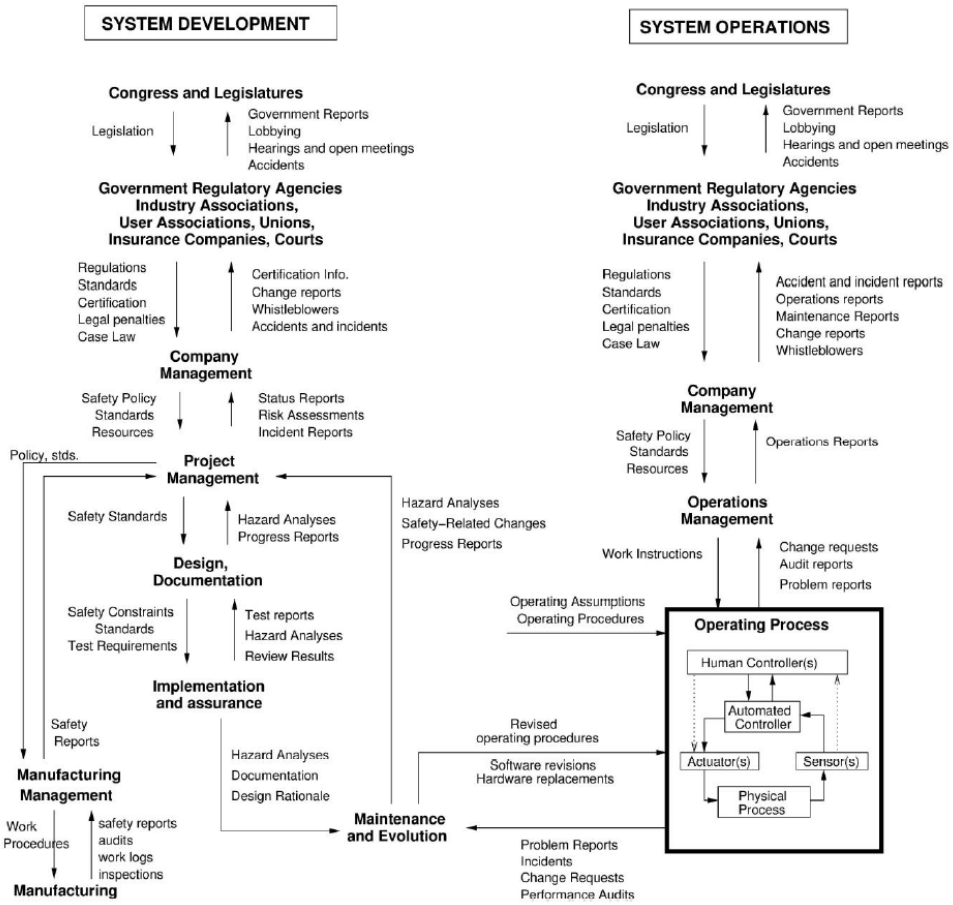
배경지식 – STAMP/STPA

- STAMP
  - System-Theoretic Accident Model and Process

- STAMP는 하드웨어와 소프트웨어뿐만 아니라 운영적인 요소, 환경을 포함한 다양한 구성요소를 계층적으로 표현

- Control structure는 전체 시스템을 표현하며, 여러 Control loop의 조합을 가짐





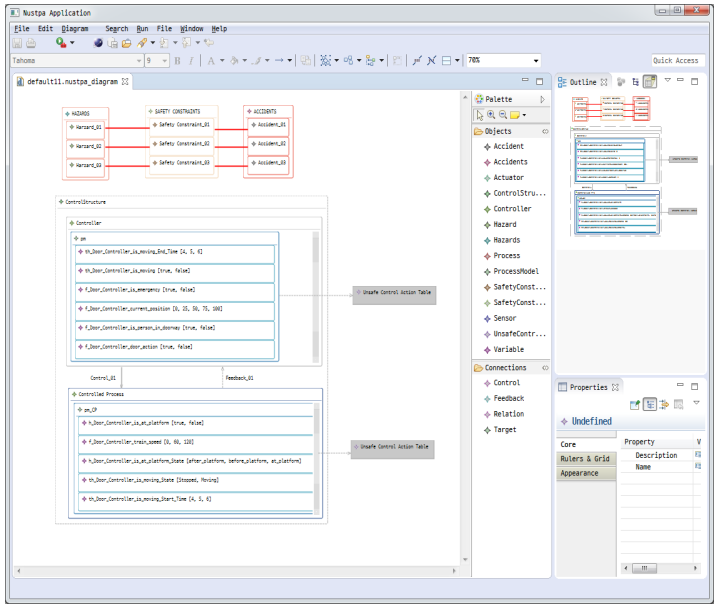
배경지식 – STAMP/STPA

- STPA (System-Theoretic Process Analysis) 기법은 STAMP에 기반한 안전성 분석기법
- STAMP 모델에서 표현된 개별 시스템 혹은 컴포넌트의 정상 작동에도 불구하고 Control/Feedback과 같은 상호작용에 의해 위험이 발생할 수 있음
- STPA 안전성 분석 기법의 결과는 시스템을 위험하게 만드는 Unsafe Control Action (UCA) 의 발견 및 Unsafe Control Action의 원인 분석
- STPA 수행 단계

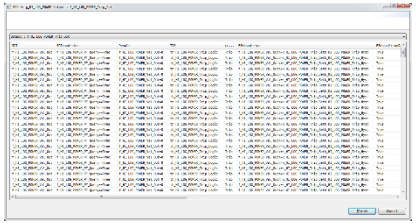
NuSTPA

S1. 사고, 위험, 제약사항 정의 → S2. Control Structure 도출 → S3. UCA도출 → S4. UCA의 원인 도출

NuSTPA Editor (NuSCR)

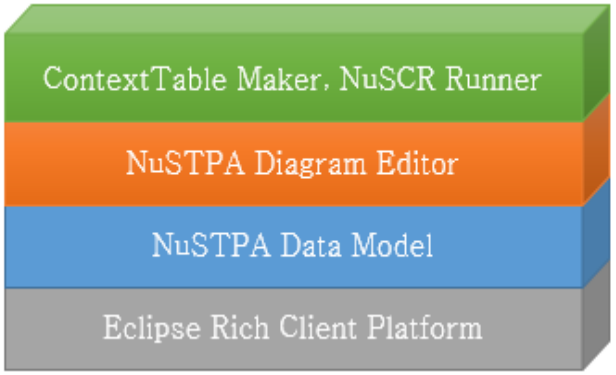


CTMaker & NuSCRRunner



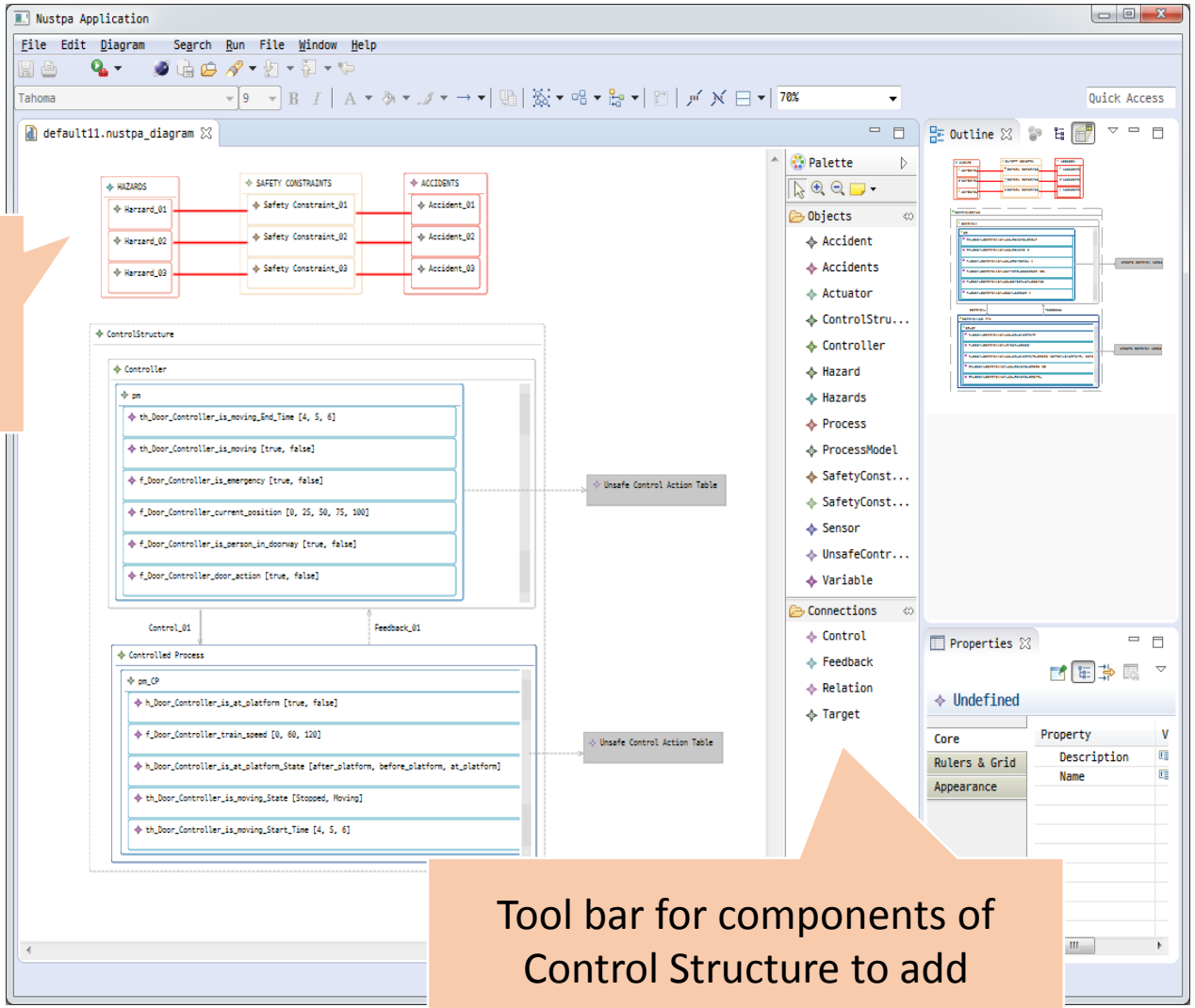
NuSTPA - NuSTPA의 구조

- Eclipse Rich Client Platform을 기반으로 개발한 도구
- Data Model : STPA 분석 수행에 필요한 데이터
- NuSTPA Diagram Editor : STPA 분석을 수행하기 위한 편집기
- ContextTable Maker, NuSCR Runner : NuSCR로 명세된 Process Model을 사용해 STPA S3에 해당하는 Unsafe Control Action 자동으로 도출



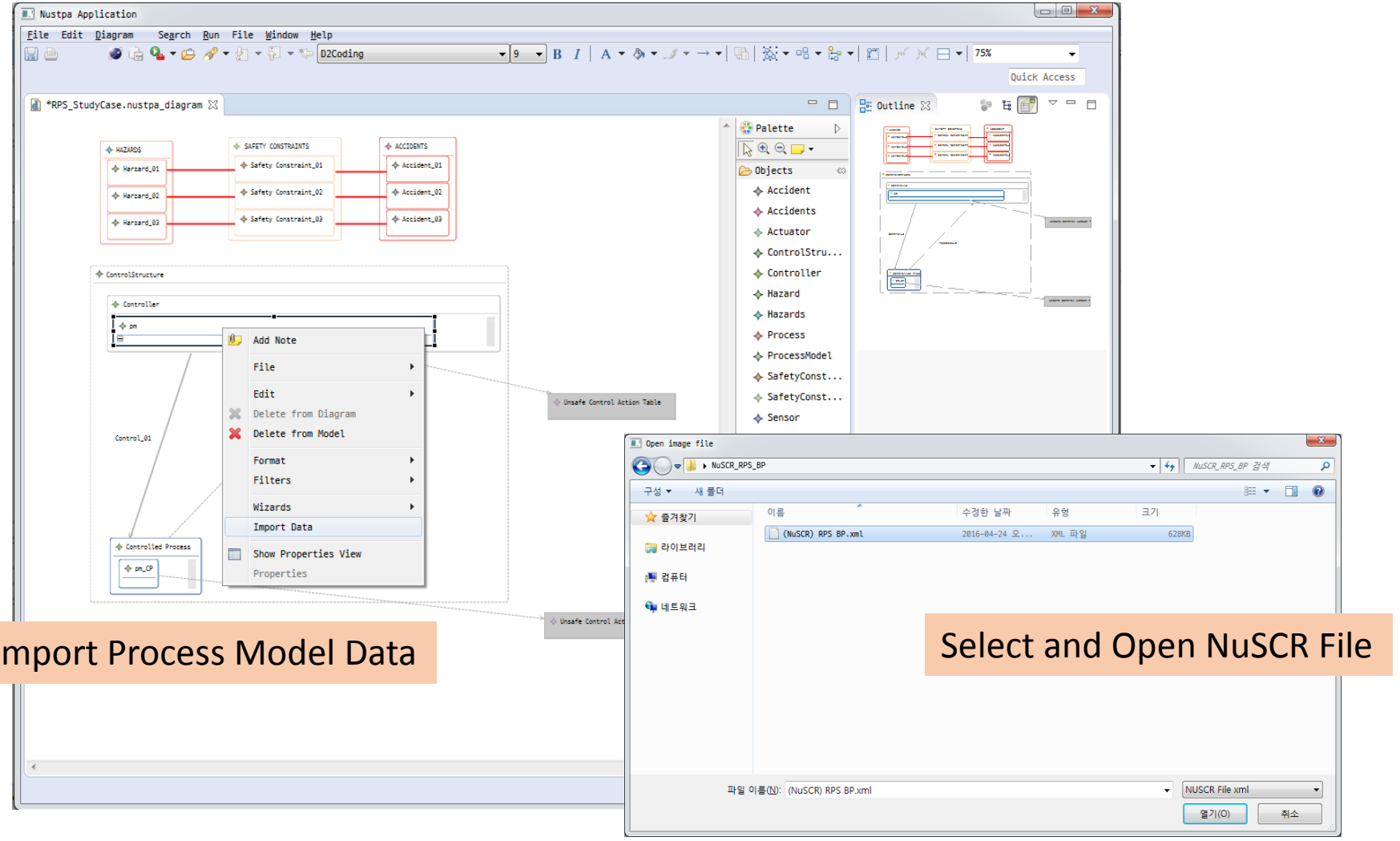
NuSTPA Diagram Editor

Graphical editor for Control Structure



Tool bar for components of Control Structure to add

NuSTPA – NuSTPA 적용

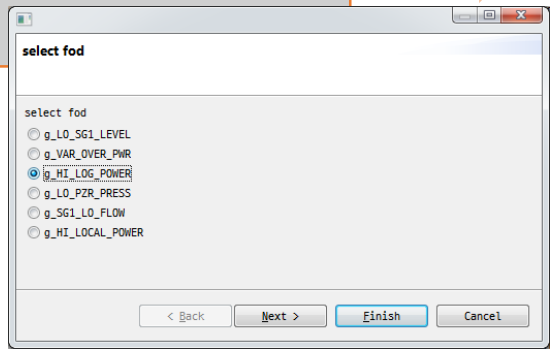


Import Process Model Data

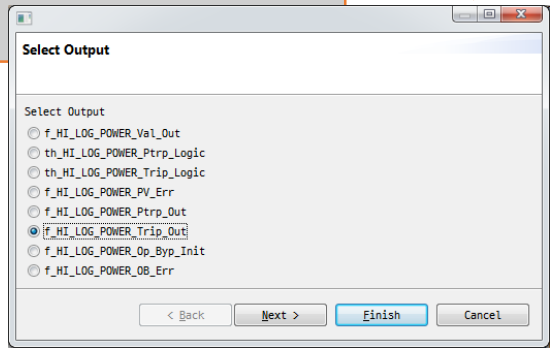
Select and Open NuSCR File

NuSTPA – NuSTPA 적용

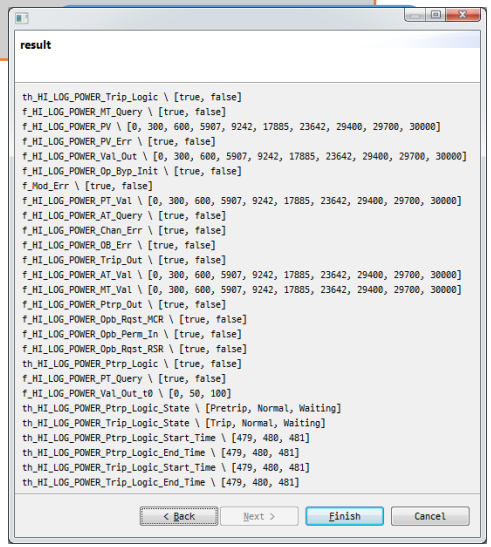
Select FOD



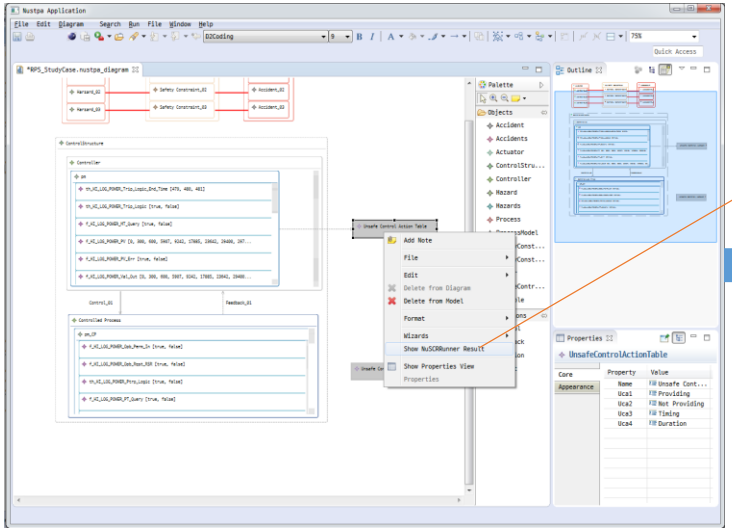
Select Output



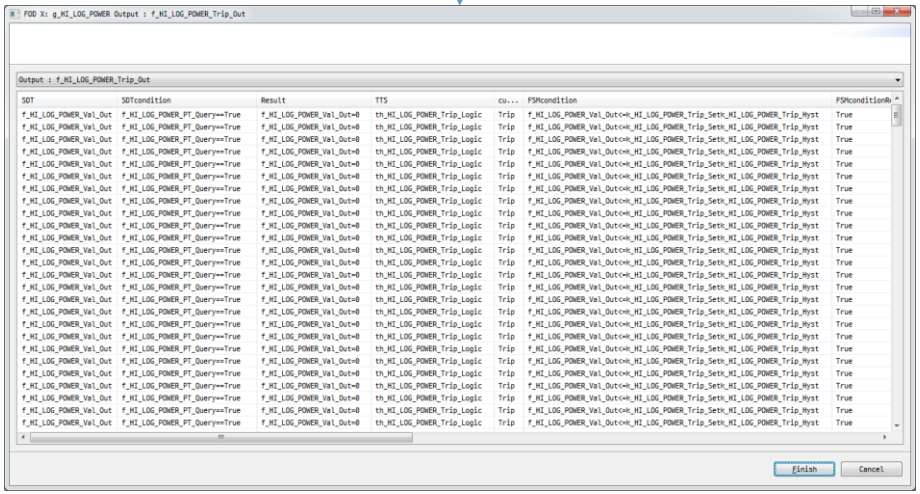
Can find and add variable o f Process Model



NuSTPA – NuSTPA 적용



Control Action in Controller



결론

- STPA의 일부 자동화를 지원하기 위한 도구인 NuSTPA를 소개
- STPA의 모든 단계를 하나의 도구에서 지원
- 분석 비용이 많이 들어가는 일부 단계를 자동화
- 향후 연구는 비안전 제어를 도출하는 개수를 줄이는 연구