NuSTPA 2.0: A Tool to Perform the STPA Using NuSCR Formal Specification

NuSCR 정형명세 언어를 사용하는 STPA 지원 도구 개발

허윤아 정세진 유준범

Dependable Software Laboratory

Konkuk University

2021.12.21

목차

- Introduction
- NuSCR
  - NuFTA
- An overview of NuSTPA 2.0
- Conclusion and Future work

Introduction

- Hazard Analysis
  - Hazard를 식별하고 줄이기 위해서 safety-critical systems에 대해 수행

- STPA
  - **S**ystems-**T**heoretic **P**rocess **A**nalysis
  - Hazard analysis technique
  - **S**ystems-**T**heoretic **A**ccident **M**odel and **P**rocesses (STAMP) 라는 accident model에 기반함
  - 주로 manual하게 수행 & 분석가의 경험에 의존

  → 수행하는 데에 많은 시간과 노력이 필요

- **NuSTPA 2.0**
  - STPA + formal approach + tool
  - STPA를 좀 더 효율적으로 수행하기 위해
  - **NuSCR formal specification을 이용한 formal approach를 통해 STPA process를 지원**

Introduction

- STPA process

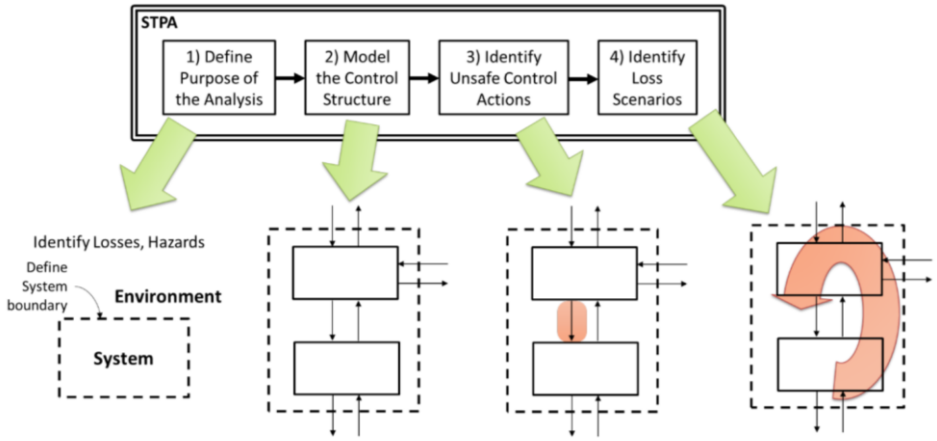
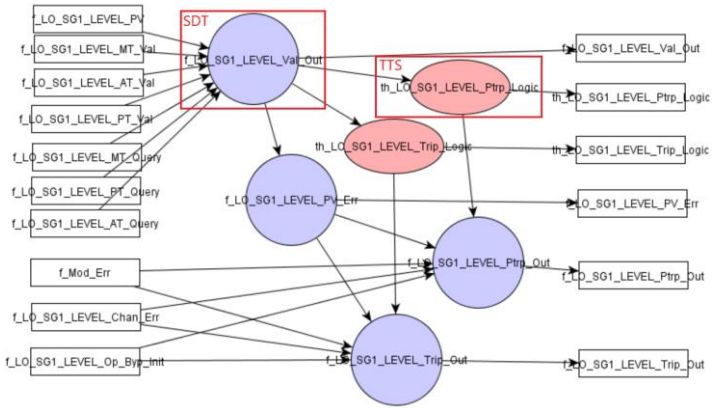


Figure 2.1: Overview of the basic STPA Method

- Loss: 시스템에 발생 가능한 손실
- Hazard: loss의 원인
- Control structure: control loop으로 구성된 시스템의 추상적 모델
- Unsafe Control Action (UCA): 특정 context에서 hazard를 일으킬 수 있는 control action
- Loss scenario: UCA와 hazard를 발생시킬 수 있는 causal factors

NuSCR

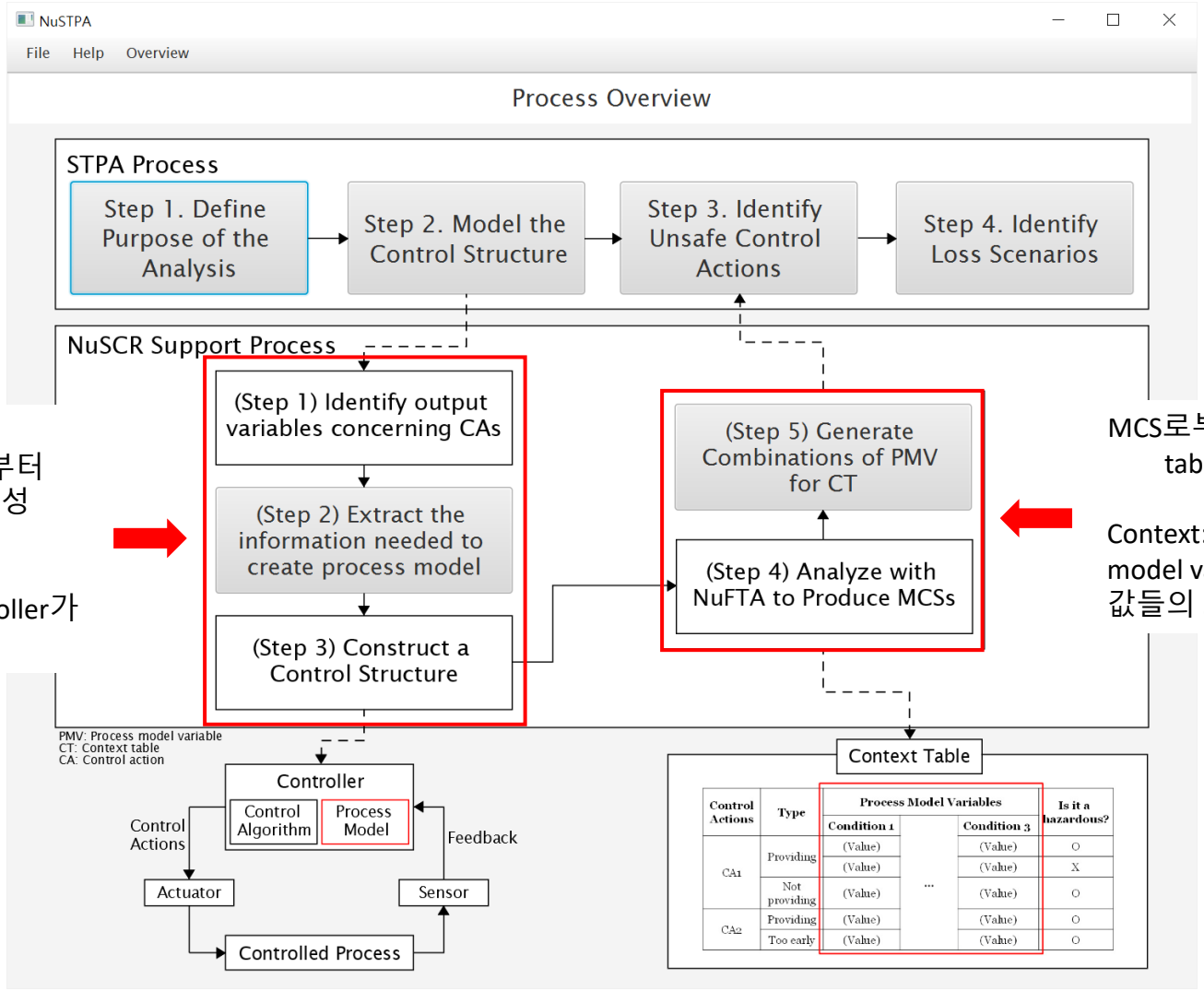
- Formal software requirements specification method
- 원자력 발전소의 digital plant protection system의 specification을 작성하기 위함
- Function Overview Diagrams (FODs)으로 구성
  - Data flow를 보이기 위한 system components & dependencies의 overview
  - Structure Decision Table (SDT), Finite State Machine (FSM), Timed Transition System (TTS) 노드로 구성
  - 각 노드는 연관된 노드와 input/output variable들에 연결



NuSCR specification의 <g_LO_SG1_LEVEL> 모듈

- NuFTA
  - NuSCR에 대해 fault tree analysis를 수행하기 위한 도구
  - Fault tree를 그리고 minimal cut-set (MCS)를 생성
  - MCS: fault tree의 top event에 도달하기 위한 기본 이벤트들의 최소한의 집합

An overview of NuSTPA 2.0



NuSCR specification으로부터 process model 생성

Process model: CA를 제공하기 위해 controller가 가지고 있는 값

MCS로부터 context table 생성

Context: process model variable의 값들의 조합

NuSTPA 2.0의 메인 화면

An overview of NuSTPA 2.0

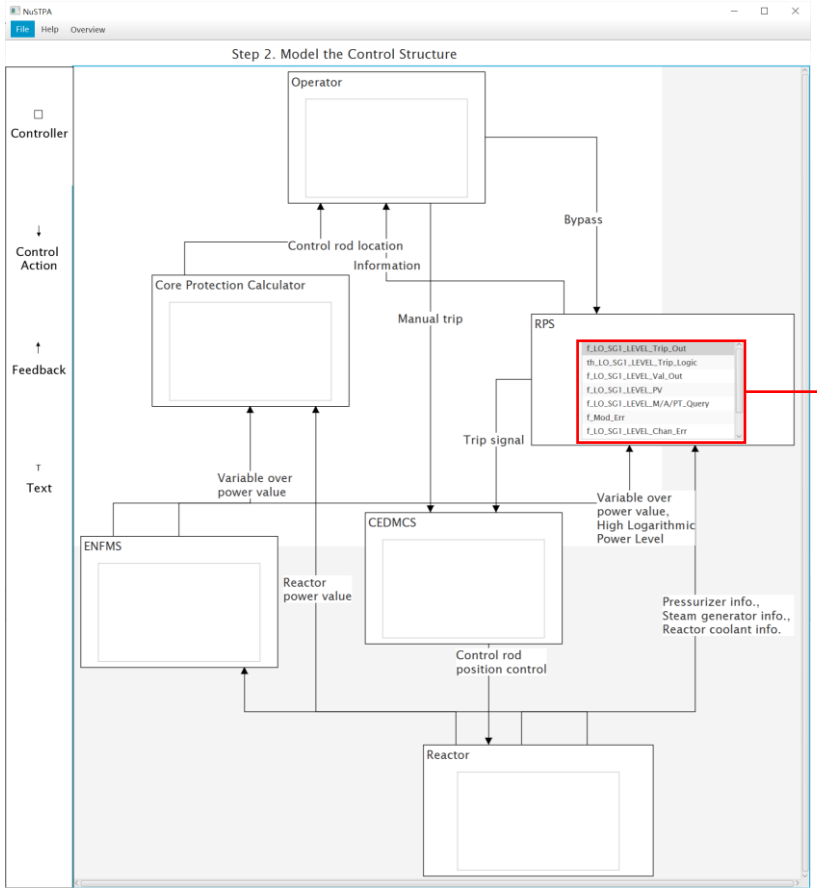
- NuSTPA 2.0의 요구사항

Req. 1	Control structure를 그릴 수 있어야 하고 각각의 process model을 보여줄 수 있어야 한다.
Req. 2	Process model 변수를 자동으로 생성하기 위해서 NuSCR 파일을 parsing할 수 있어야 한다. 또한 각 FOD와 그 내부의 변수들과 각 노드들을 식별할 수 있어야 한다.
Req. 3	Process model 변수와 그 값은 manual하게 더해질 수 있어야 한다. 생성된 process model 변수는 삭제되거나 수정되거나 추상화될 수 있어야 한다.
Req. 4	Context table을 자동으로 생성하기 위해서 MCS 파일을 parsing할 수 있어야 한다.
Req. 5	Context table의 context는 manual하게 더해질 수 있어야 한다. Context table의 각 아이템은 수정되거나 삭제될 수 있어야 한다.
Req. 6	UCA table을 context table로부터 자동으로 생성할 수 있어야 한다. UCA table은 control action을 unsafe하도록 만드는 context들만 보여줘야 한다.

An overview of NuSTPA 2.0

- Req. 1 - Control structure를 그릴 수 있어야 하고 각각의 process model을 보여줄 수 있어야 한다.

  → Control structure를 그리기 위한 editor를 제공함



[Trip signal] Control Action을 제공하기 위한 process model

'RPS' controller에 대한 control structure

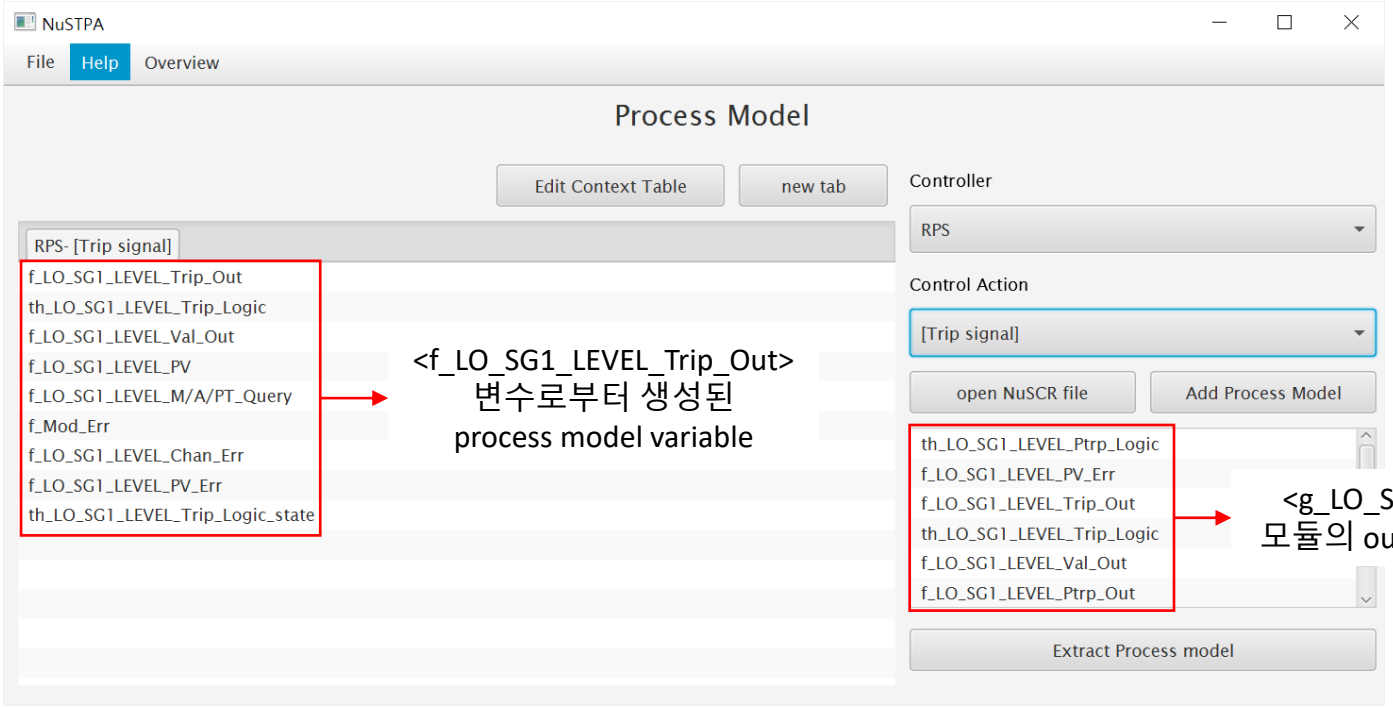
An overview of NuSTPA 2.0

- Req. 2 - Process model 변수를 자동으로 생성하기 위해서 NuSCR 파일을 parsing할 수 있어야 한다. 또한 각 FOD와 그 내부의 변수들과 각 노드들을 식별할 수 있어야 한다.

  → **DOM xpath parser**를 이용해 NuSCR 파일을 parsing하고 각각에 대한 ArrayList를 생성
  - 이전 연구에서 제안된 <Extracting Variable Information> 알고리즘을 따름

- Req. 3 - Process model 변수와 그 값은 manual하게 더해질 수 있어야 한다. 생성된 process model 변수는 삭제되거나 수정되거나 추상화될 수 있어야 한다.

  → Javafx의 text field, context menu 활용



'RPS' controller에 대한 process model

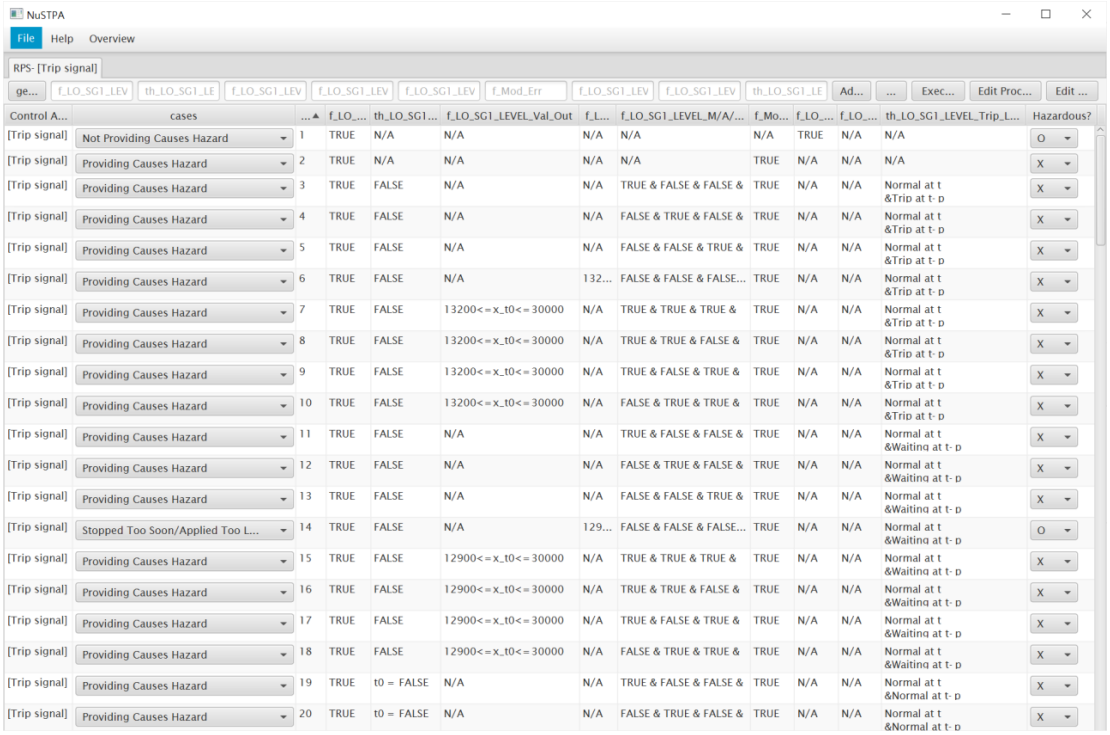
An overview of NuSTPA 2.0

- Req. 4 - Context table을 자동으로 생성하기 위해서 MCS 파일을 parsing할 수 있어야 한다.

  → **bufferedReader**를 이용해 MCS 파일을 parsing함
  - 이전 연구에서 제안된 <Generating Context Table> 알고리즘을 따름

- Req. 5 - Context table의 context는 manual하게 더해질 수 있어야 한다. Context table의 각 아이템은 수정되거나 삭제될 수 있어야 한다.

  → javafx의 context menu, text field, table cell editing 기능 활용

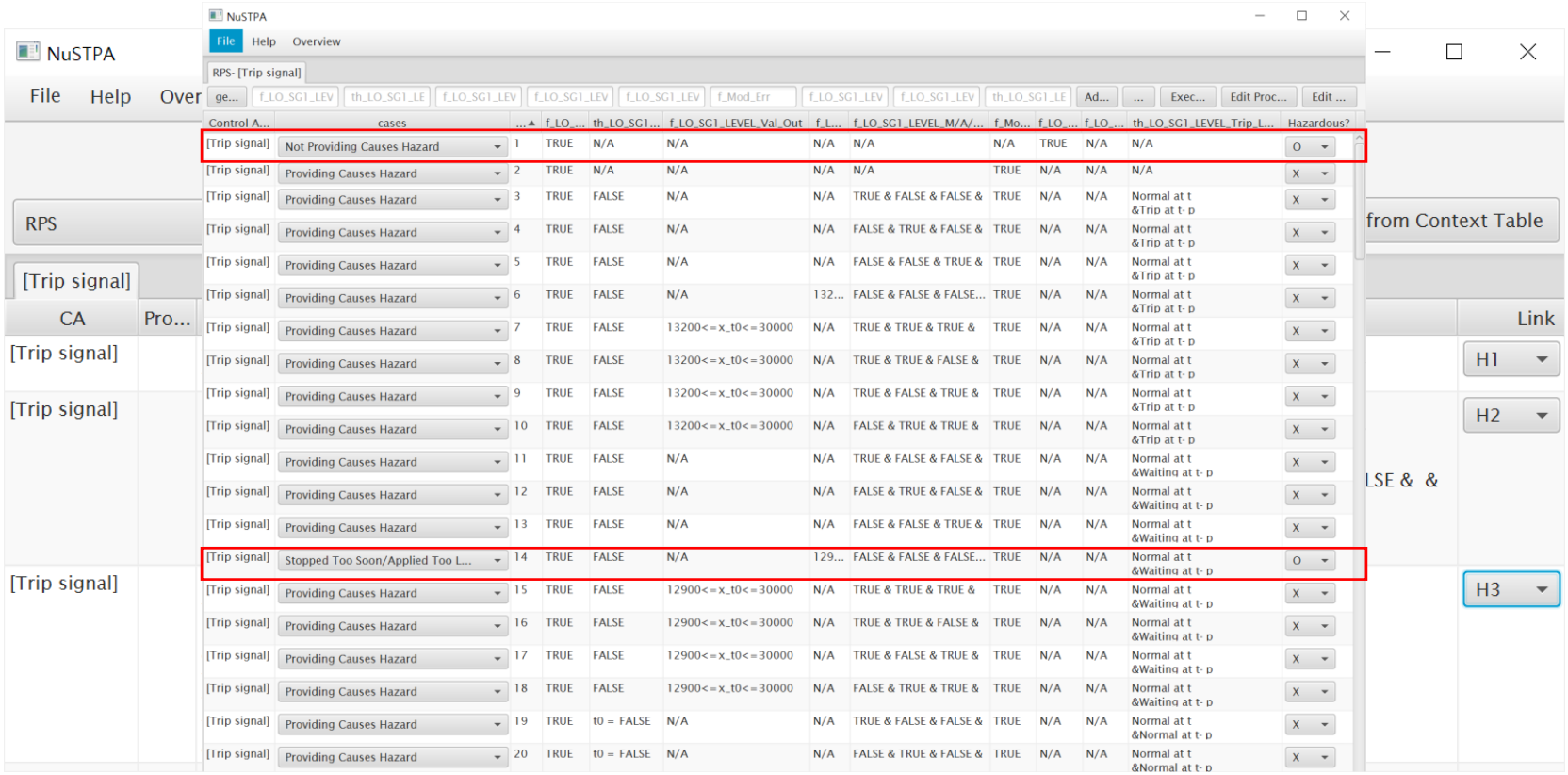


Control A...	cases	...	f_LO_...	th_LO_SG1...	f_LO_SG1_LEVEL_Val_Out	f_L...	f_LO_SG1_LEVEL_M/A/...	f_Mo...	f_LO_...	f_LO_...	th_LO_SG1_LEVEL_Trip_L...	Hazardous?
[Trip signal]	Not Providing Causes Hazard	1	TRUE	N/A	N/A	N/A	N/A	N/A	TRUE	N/A	N/A	O
[Trip signal]	Providing Causes Hazard	2	TRUE	N/A	N/A	N/A	N/A	TRUE	N/A	N/A	N/A	X
[Trip signal]	Providing Causes Hazard	3	TRUE	FALSE	N/A	N/A	TRUE & FALSE & FALSE &	TRUE	N/A	N/A	Normal at t &Trip at t- p	X
[Trip signal]	Providing Causes Hazard	4	TRUE	FALSE	N/A	N/A	FALSE & TRUE & FALSE &	TRUE	N/A	N/A	Normal at t &Trip at t- p	X
[Trip signal]	Providing Causes Hazard	5	TRUE	FALSE	N/A	N/A	FALSE & FALSE & TRUE &	TRUE	N/A	N/A	Normal at t &Trip at t- p	X
[Trip signal]	Providing Causes Hazard	6	TRUE	FALSE	N/A	132...	FALSE & FALSE & FALSE...	TRUE	N/A	N/A	Normal at t &Trip at t- p	X
[Trip signal]	Providing Causes Hazard	7	TRUE	FALSE	13200<=x_t0<=30000	N/A	TRUE & TRUE & TRUE &	TRUE	N/A	N/A	Normal at t &Trip at t- p	X
[Trip signal]	Providing Causes Hazard	8	TRUE	FALSE	13200<=x_t0<=30000	N/A	TRUE & TRUE & FALSE &	TRUE	N/A	N/A	Normal at t &Trip at t- p	X
[Trip signal]	Providing Causes Hazard	9	TRUE	FALSE	13200<=x_t0<=30000	N/A	TRUE & FALSE & TRUE &	TRUE	N/A	N/A	Normal at t &Trip at t- p	X
[Trip signal]	Providing Causes Hazard	10	TRUE	FALSE	13200<=x_t0<=30000	N/A	FALSE & TRUE & TRUE &	TRUE	N/A	N/A	Normal at t &Trip at t- p	X
[Trip signal]	Providing Causes Hazard	11	TRUE	FALSE	N/A	N/A	TRUE & FALSE & FALSE &	TRUE	N/A	N/A	Normal at t &Waiting at t- p	X
[Trip signal]	Providing Causes Hazard	12	TRUE	FALSE	N/A	N/A	FALSE & TRUE & FALSE &	TRUE	N/A	N/A	Normal at t &Waiting at t- p	X
[Trip signal]	Providing Causes Hazard	13	TRUE	FALSE	N/A	N/A	FALSE & FALSE & TRUE &	TRUE	N/A	N/A	Normal at t &Waiting at t- p	X
[Trip signal]	Stopped Too Soon/Applied Too L...	14	TRUE	FALSE	N/A	129...	FALSE & FALSE & FALSE...	TRUE	N/A	N/A	Normal at t &Waiting at t- p	O
[Trip signal]	Providing Causes Hazard	15	TRUE	FALSE	12900<=x_t0<=30000	N/A	TRUE & TRUE & TRUE &	TRUE	N/A	N/A	Normal at t &Waiting at t- p	X
[Trip signal]	Providing Causes Hazard	16	TRUE	FALSE	12900<=x_t0<=30000	N/A	TRUE & TRUE & FALSE &	TRUE	N/A	N/A	Normal at t &Waiting at t- p	X
[Trip signal]	Providing Causes Hazard	17	TRUE	FALSE	12900<=x_t0<=30000	N/A	TRUE & FALSE & TRUE &	TRUE	N/A	N/A	Normal at t &Waiting at t- p	X
[Trip signal]	Providing Causes Hazard	18	TRUE	FALSE	12900<=x_t0<=30000	N/A	FALSE & TRUE & TRUE &	TRUE	N/A	N/A	Normal at t &Waiting at t- p	X
[Trip signal]	Providing Causes Hazard	19	TRUE	t0 = FALSE	N/A	N/A	TRUE & FALSE & FALSE &	TRUE	N/A	N/A	Normal at t &Normal at t- p	X
[Trip signal]	Providing Causes Hazard	20	TRUE	t0 = FALSE	N/A	N/A	FALSE & TRUE & FALSE &	TRUE	N/A	N/A	Normal at t &Normal at t- p	X

'Trip Signal' CA에 대한 context table

An overview of NuSTPA 2.0

- Req. 6 - UCA table을 context table로부터 자동으로 생성할 수 있어야 한다. UCA table은 control action을 unsafe하도록 만드는 context들만 보여줘야 한다.



'Trip Signal' CA에 대한 UCA table

Conclusion and Future work

- NuSTPA 2.0: NuSCR formal specification을 통해 지원되는 STPA process를 적용하기 위한 도구

- NuSTPA 2.0은…
  - Control structure를 그리기 위한 editor를 지원
  - NuSCR specification으로부터 process model을 자동으로 생성
  - MCS로부터 context table을 자동으로 생성
  - Context table로부터 UCA table을 자동으로 생성

- 향후 연구
  - Context table과 UCA table을 생성하는 알고리즘과 Control structure editor의 알고리즘 개선
  - 계층적인 control structure을 그려서 시스템을 분석할 수 있도록 함
  - 전체 프로세스의 traceability를 보일 수 있도록 함

KU KONKUK UNIVERSITY

감사합니다.

Q&A

허윤아
hya1202@konkuk.ac.kr
https://dslab.konkuk.ac.kr

DS DEPENDABLE SOFTWARE LABORATORY