요구사항분석

STPA기반 위험 분석 개발 지원도구

T5
201510436 허윤아
201611261 민지호
201614158 장다혜
201611293 전다윤
201710515 최연지

Functional Requirement

1. 사용자가 Editor를 통해 Control Structure를 모델링할 수 있어야 한다.
1-1. System의 SW controller에는 동작을 결정하는 정보(System error, system state, environment 등)가 포함되어야 한다.
1-2. Control Structure를 작성할 때 Control Action과 Feedback을 구체적으로 작성할 수 있어야 한다.

2. 모델링한 Control Structure가 정형명세 언어인 NuSCR을 지원해야 한다.
2-1. NuSCR로 작성된 SW formal specification을 활용하여 STPA를 지원할 수 있어야 한다.
2-1-1. NuSCR로 작성된 파일을 불러올 수 있다.
2-1-2. 불러온 파일을 통해 NuSCR을 파싱하여, 분석하려는 CA(control action)와 연관된 output variable 을 추출한다.
2-1-3. output variable 추출에 필수적인 input variable, internal variable 추출한다.
2-1-4. 위의 결과로 추출된 모든 변수들을 이용해 controller별 process variable 및 model 을 생성한다.

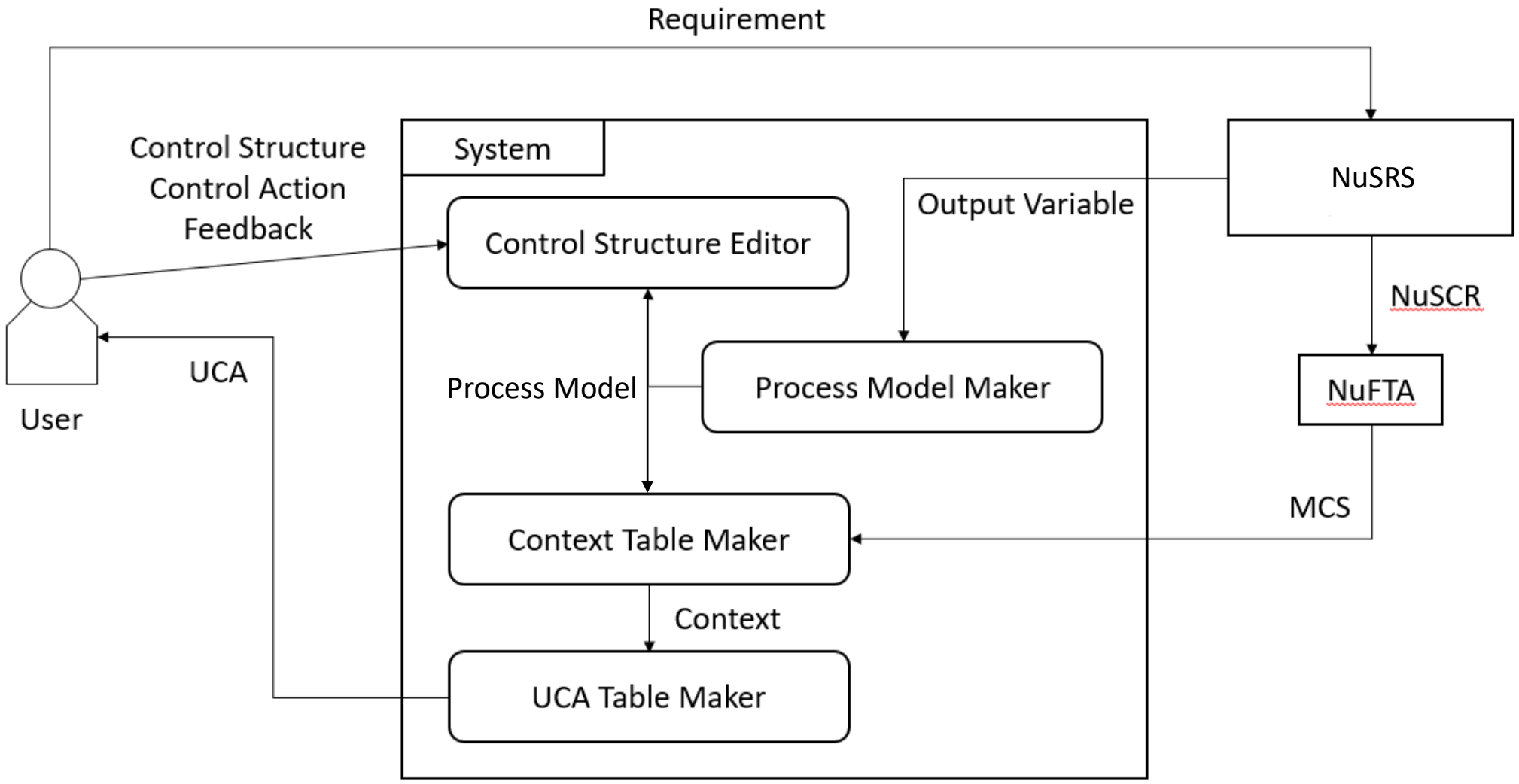
2-2. NuFTA를 통해 추출된 MCS(minimal cut-set)를 이용해 context table을 생성한다.
2-2-1. NuSCR를 NuFTA를 통해 Backward-analysis한 결과를 통해 MCS가 추출되면, 이 중 유의미한 값을 추출한다.

3. Unsafe Control Actions을 통해 loss scenario를 분석할 수 있어야 한다.
3-1. 2-2에서 생성된 context table을 기반으로 Controller 별 CA 에 따라 UCA 후보군을 생성한다.
3-1-1. UCA = Controller & Type & Control Action & Context [Link to Hazards]
3-2. 생성된 UCA 후보군에 대해 loss scenario를 분석할 수 있도록 table로 정리되어야 한다.

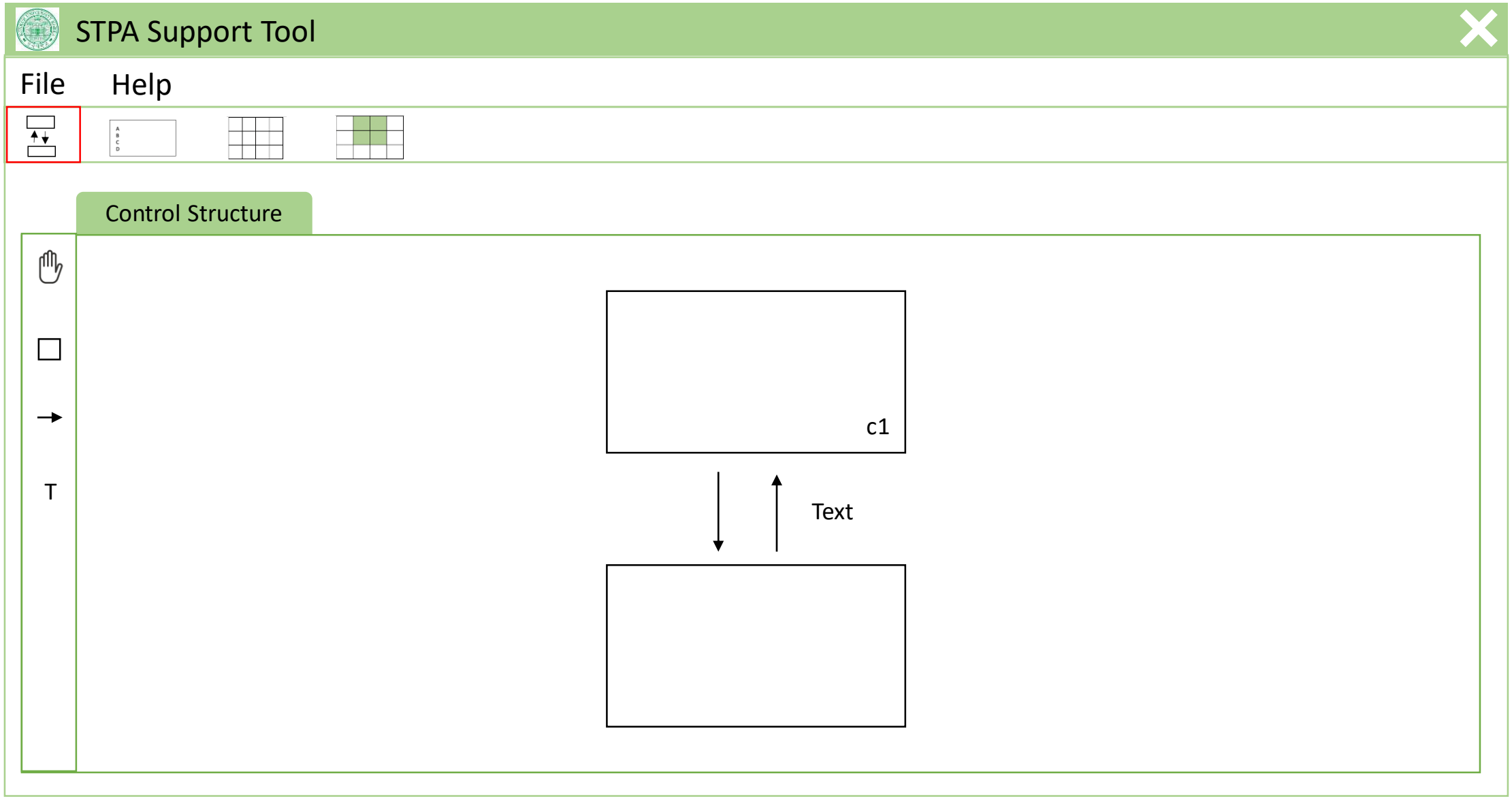
Non-Functional Requirement

1. 사용자가 쓰기에 편리하고 직관적인 UI를 만든다.
2. 시스템의 종류에 관계없이, 범용적으로 사용할 수 있는 프로그램이여야 한다.

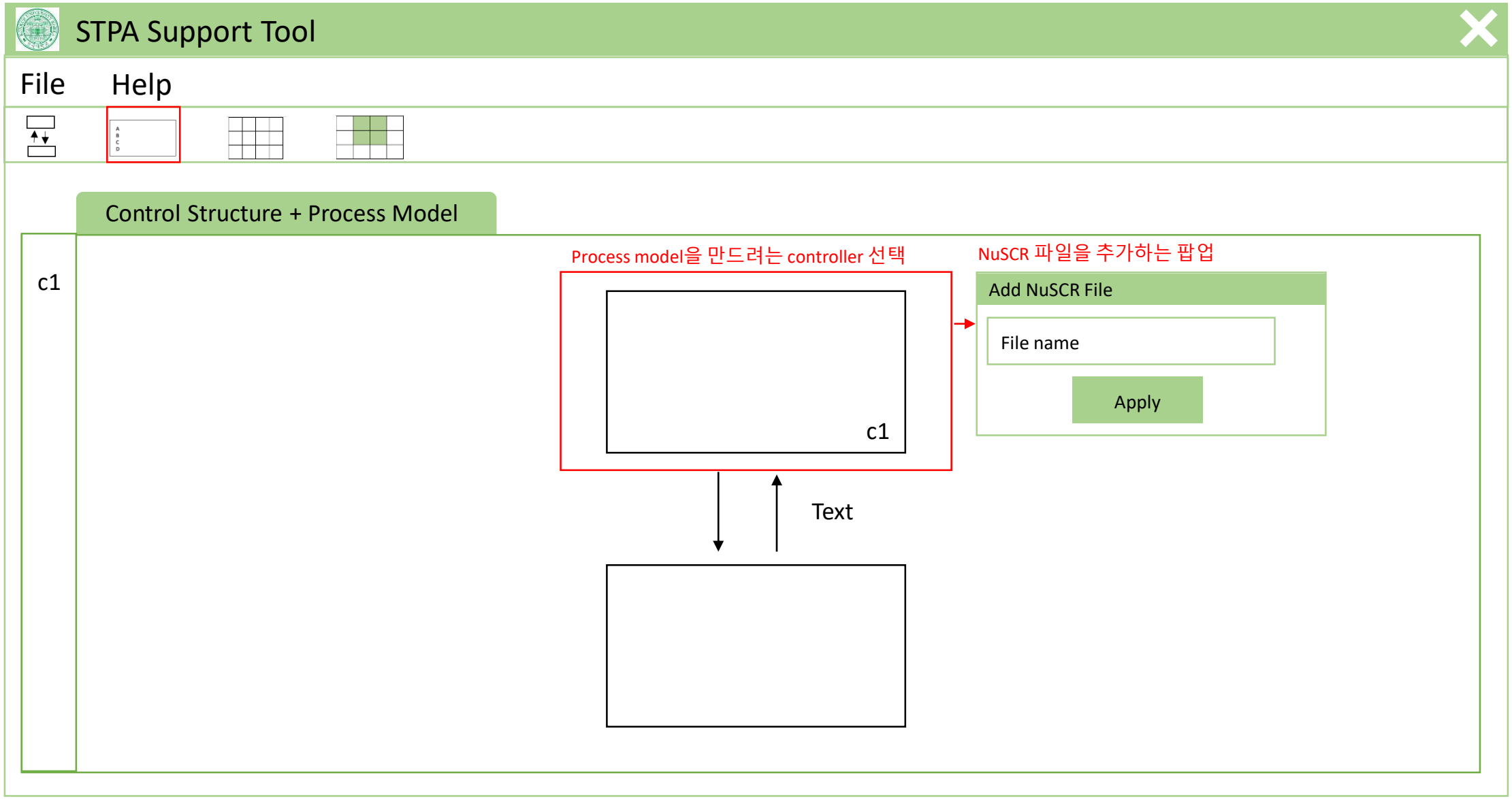
Architecture Diagram



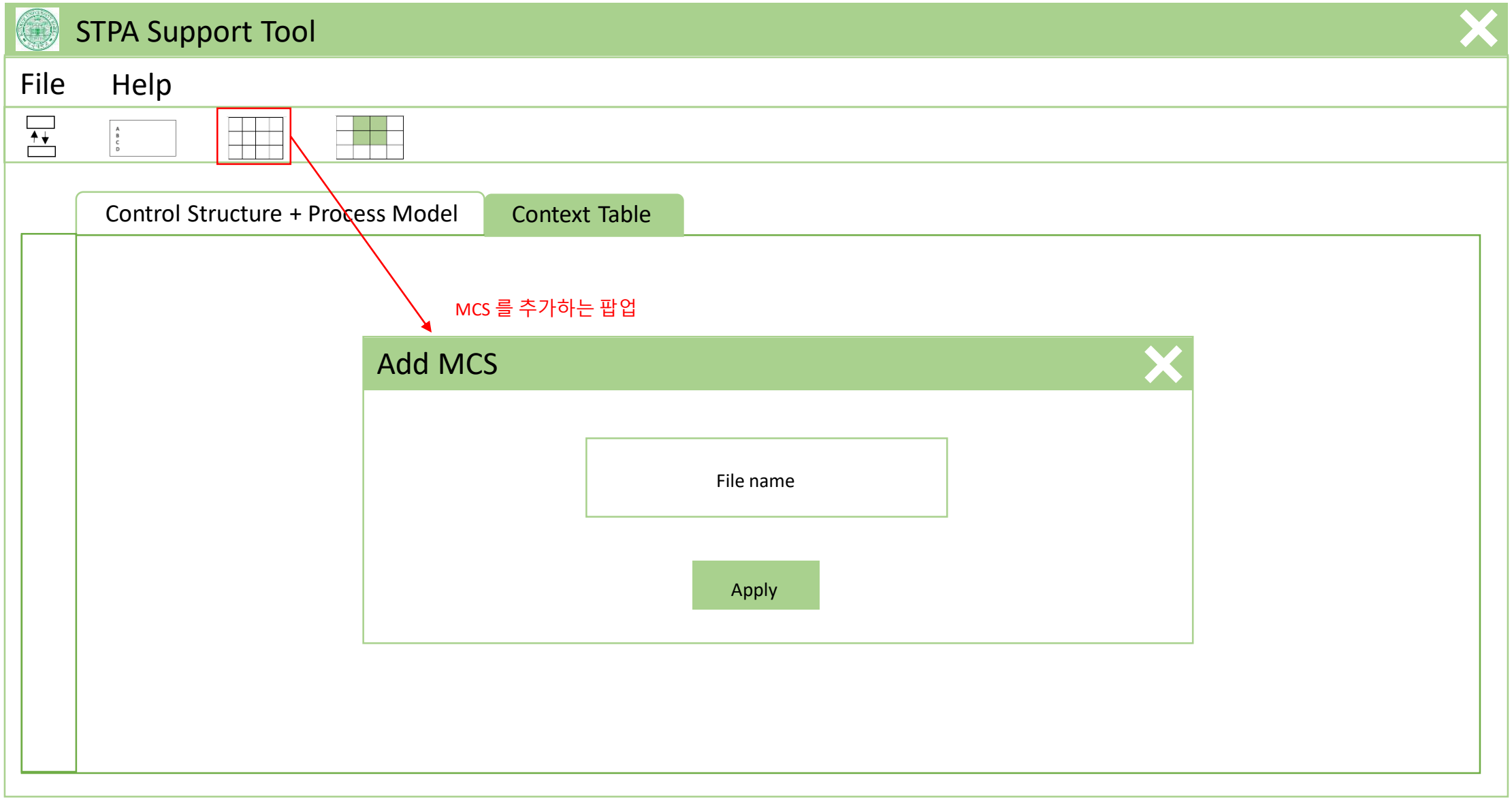
Control Structure Editor UI



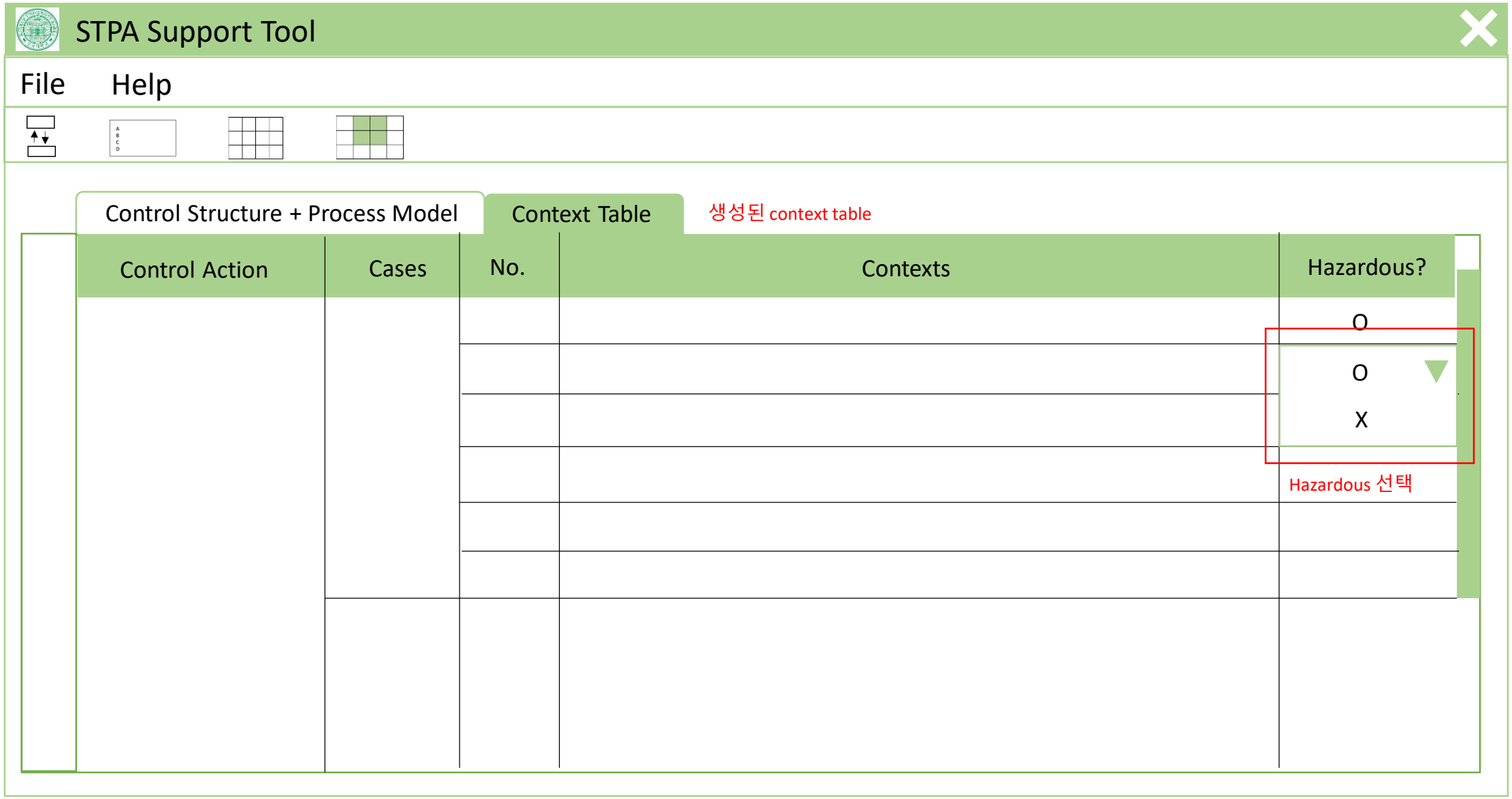
Control Structure Editor UI



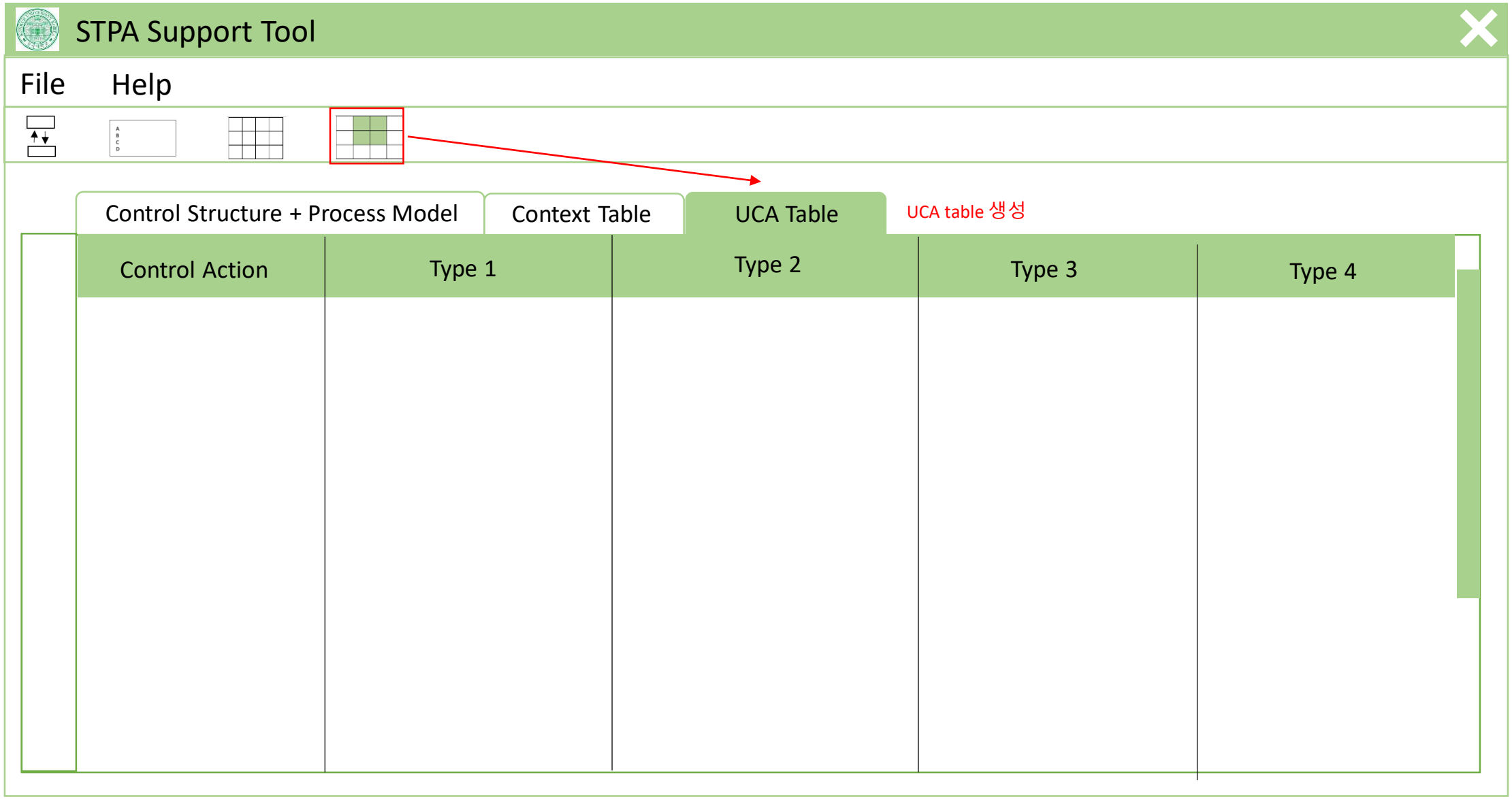
Process Model Maker UI



Process Model Maker UI



Process Model Maker UI



System Test Case

Requirement	Test case	Success Criteria
1-1	System의 SW controller에는 동작을 결정하는 정보(System error, system state, environment 등)가 포함되는지 여부를 확인	Control Structure 작성 시, System의 SW controller에는 동작을 결정하는 정보들을 함께 작성할 수 있다.
1-2	작성된 Control Action과 Feedback이 포함되는지 여부를 확인	Control Structure 작성 시, Control Action 과 Feedback을 함께 작성할 수 있다.
2-1-1	NuSCR로 작성된 파일을 불러올 수 있는지 여부를 확인	예시 NuSCR 파일(ex 원자력 발전소)을 불러올 수 있다.
2-1-2	분석하려는 CA(control action)와 연관된 output variable를 추출할 수 있는지 여부를 확인	추출된 output variable이 예상 값과 일치한다.
2-1-3	input variable, internal variable 이 output variable 추출에 필수적인지 여부를 확인	추출된 input variable, internal variable 이 예상 값과 일치한다.
2-1-4	process variable 및 model이 Controller별로 생성되었는지 여부를 확인	Process variable, model이 필요한 controller에 예상 값과 일치하게 생성된다.
2-2-1	MCS 중 유의미한 값을 추출할 수 있는지 여부를 확인	MCS에서 추출된 값들이 예상 값과 일치한다.
3-1	context table을 기반으로 Controller 별 CA 에 따라 UCA 후보군을 생성되는지 여부를 확인	생성된 UCA 후보군들이 예상 값과 일치한다.
3-1-1	UCA format에 맞게 작성되었는지 여부를 확인	UCA 후보군들이 UCA format(UCA = Controller & Type & Control Action & Context [Link to Hazards])에 맞게 작성된다.
3-2	생성된 UCA 후보군이 table로 추출되는지 여부를 확인	UCA 후보군들이 UCA table에 맞게 작성된다.