졸업프로젝트 제안서

STPA기반 위험 분석 개발 지원 도구

T5
201510436 허윤아
201611261 민지호
201614158 장다혜
201611293 전다윤

Project Description

Formal software specification language인 NuSCR로 작성된 SW를 기반으로 하는 controller system의 safety/hazard analysis를 위해 STPA를 효율적으로 수행할 수 있도록 하는 자동화 지원 도구를 개발한다.

1) Control Structure를 작성할 수 있는 editor 지원
2) NuSCR로 작성된 SW formal specification을 활용해 controller가 control action을 결정할 때 필요한 process model의 변수들 추출
3) Process model의 변수들의 조합을 통해 context table 생성
4) NuFTA를 이용해 실제로 유의미한 값들을 분석하여 생성된 context table로부터 UCA(Unsafe Control Action) 후보군 자동 생성

Project Purpose

Formal requirements specification(NuSCR)으로 작성된 SW requirement가 있는 SW-based controller 내부의 SW에 대해서, NuSCR로부터 정보를 추출해 와서 controller가 control action을 결정할 때 필요한 process model의 variable들을 작성한다.

process model의 variable들을 조합하여 context table을 작성할 수 있는데, 이것을 NuFTA를 이용해서 실제로 유의미한 값들을 분석할 수 있도록 한다.

새로 만들 SW & COTS SW/HW

새로 만들 SW 도구

• STPA 기반 위험 분석 개발 지원 도구

STPA를 기반으로 하여 NuSCR로 작성된 control structure를 modeling하고, 이를 기반으로 process model을 생성, process model의 variable들을 이용하여 context table을 만들고 NuFTA을 활용해 UCA 후보군 생성을 자동화 하는 도구

사용할 COTS SW/HW

• NuSRS 2.0, NuFTA 2.0

Project Concept

Project를 진행하면서 집중해야 할 항목들 표시

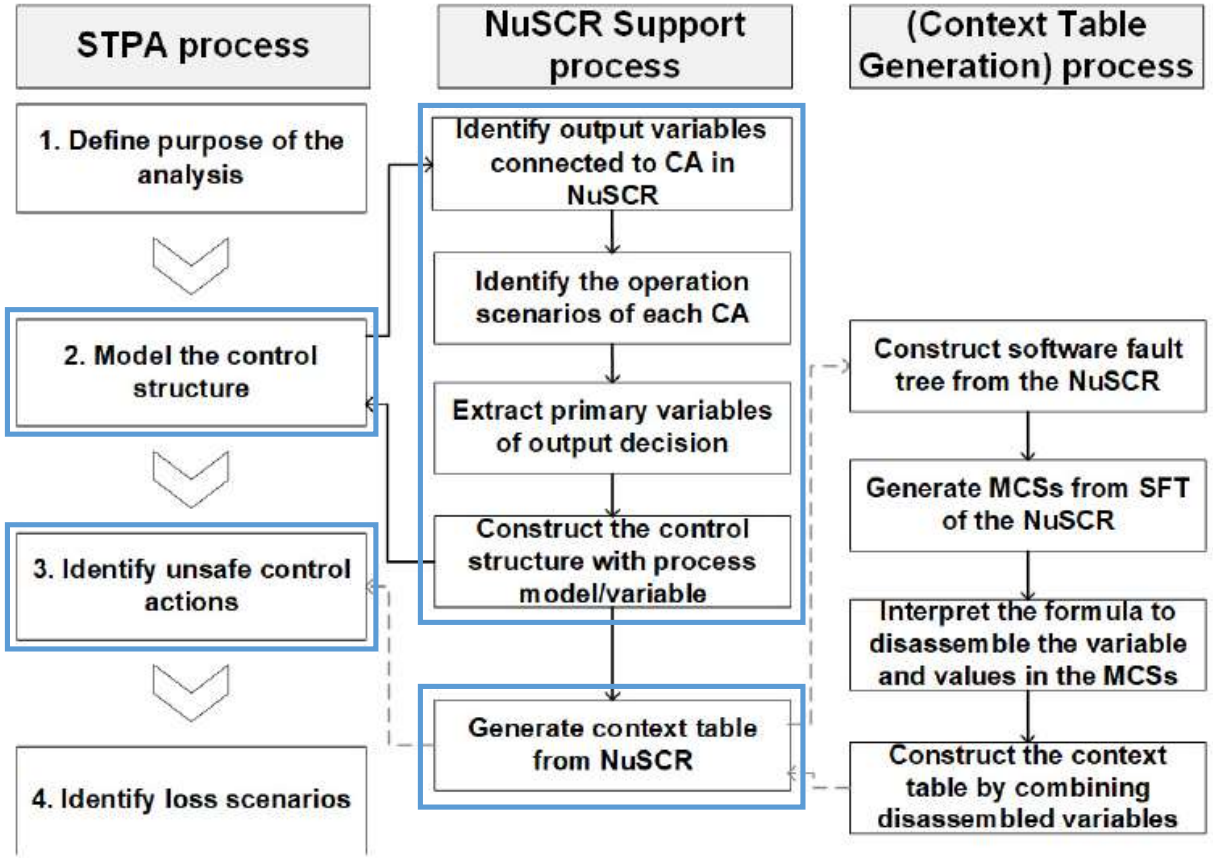


Fig. 4: Analysis process of the STPA with NuSCR supporting

Project Concept

Control Structure Model 예시

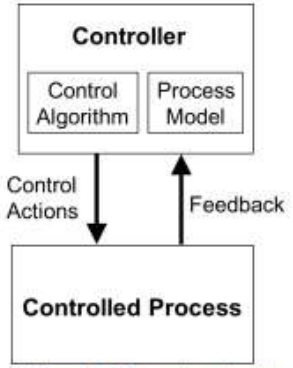


Figure 2.6: Generic control loop

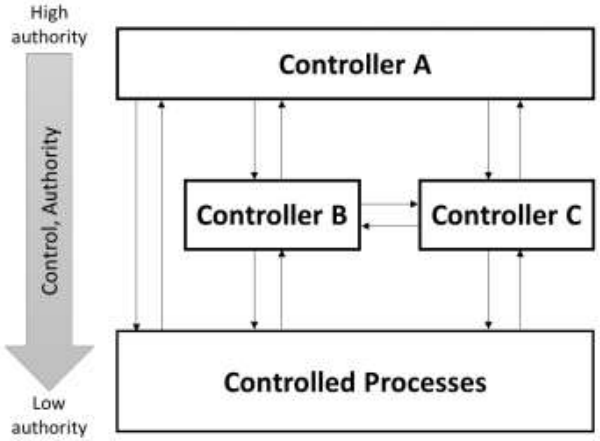


Figure 2.7: Generic hierarchical control structure

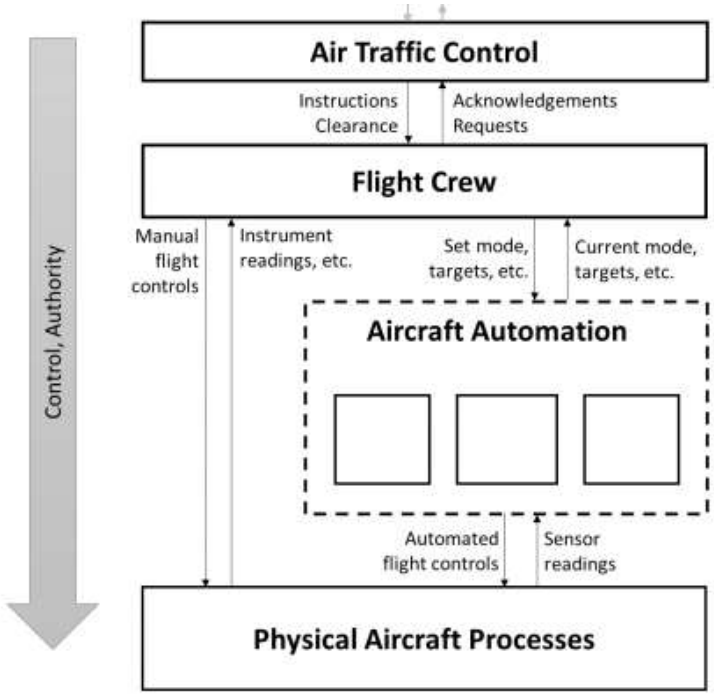
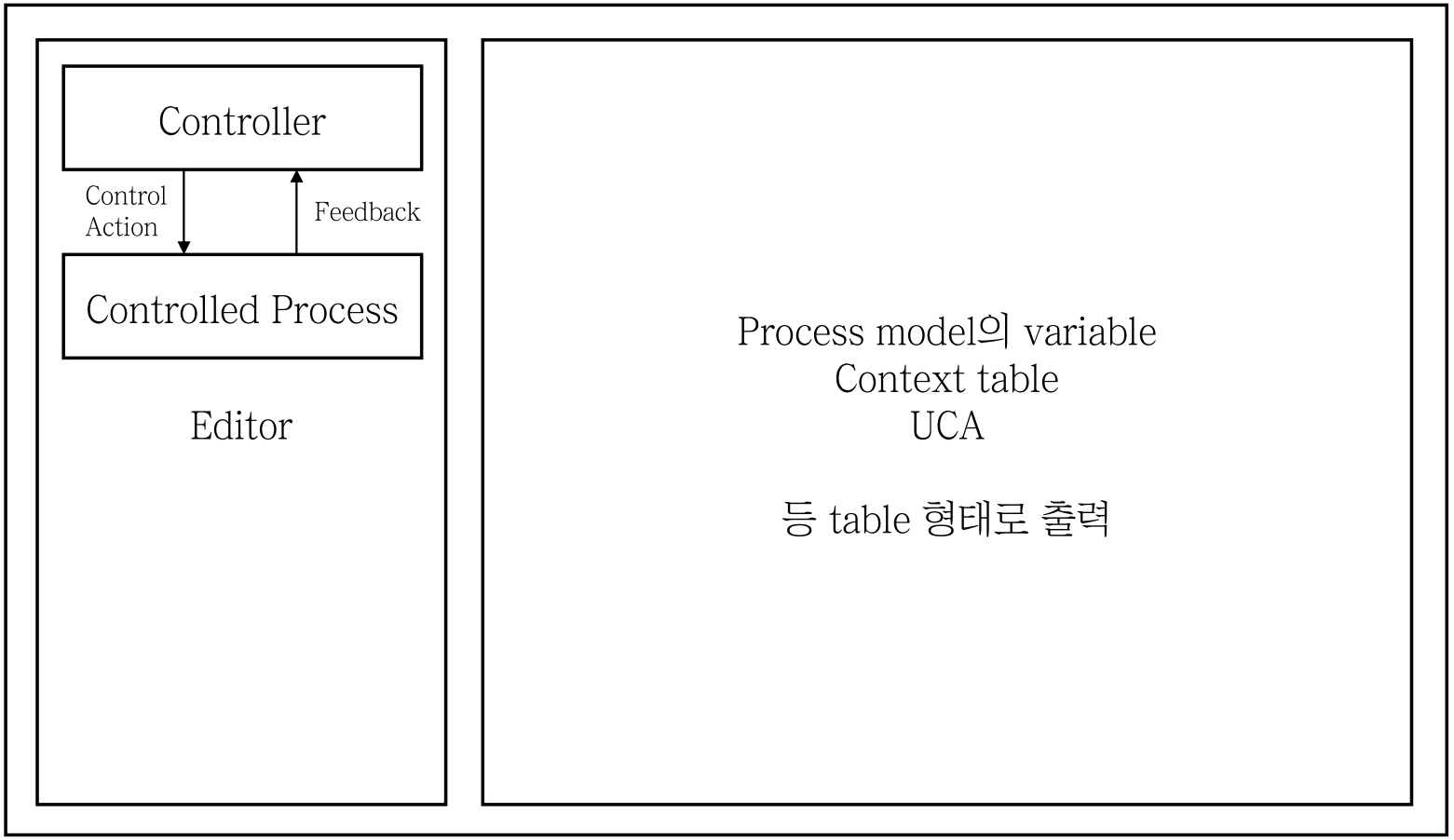


Figure 2.8: Simple example of a hierarchical control structure for aviation

최종 산출물의 기능 및 형태

1. Control structure를 작성할 때 NuSCR로부터 정보를 가져올 수 있도록 한다
2. Process model로부터 context table을 만들어낼 수 있도록 한다



대략적인 UI

Alternative Solution & Project Justification

Alternative Solution

현재 진행하려고 하는 프로젝트와 같은 목적의 도구들을 발견하지는 못했다.

Project Justification

NuSCR(requirement specification language)로 작성된 컨트롤러의 내부의 소프트웨어가 있을 때, 이 Controller는 소프트웨어에 의해서 behavior가 정해진다. 이때 STPA의 과정 중 중요한 부분인 process model의 분석과 이를 기반으로 하는 context table, 더 나아가 UCA의 생성을 지원해줌으로써 STPA를 효과적으로 수행할 수 있다.

Risk Analysis & Reduction Plan

- **STPA에 대한 지식 부족**
  : TTA에서 배포한 가이드를 참고하면서 진행

- **STPA관련 문서 탐색의 어려움**
  : 적극적인 질문과 지속적인 searching 필요

- **COTS SW에 대한 이해의 부족**
  : 프로젝트를 진행하는 기간동안 manual을 참고해가며 직접 사용

- **팀원들 간의 직접적인 소통이 어려움**
  : zoom 등의 도구를 이용한 화상 회의 진행

Success Criteria

STPA를 적용해야 하는 system이라면 종류에 무관하게 사용할 수 있는 SW를 만드는 것이 최종 목표이다.

예시로 주어진 원자력 발전소에 대해, NuSCR을 이용해 control structure를 작성하고, 이를 통해 추출된 process model과 context table, 더 나아가 NuFTA를 적용했을 때 각 변수들의 상태에 따라 UCA가 알맞게 추출되는지 확인함으로써 개발한 SW에 대한 테스트를 진행한다.