

# HyTech를 이용한 ECML 모델의 검증 및 분석

윤상현(건국대), 조재연(한양대), 전인걸(ETRI), 유준범(건국대)

2014.02.13

# 차례

- 서론
- 배경지식
  - ECML (ETRI CPS Modeling Language)
  - HyTech와 선형 하이브리드 오토마타
- ECML 모델의 선형 하이브리드 오토마타 변환
- 사례연구
- 결론

# 서론

- 하이브리드 시스템
  - 연속시스템과 이산시스템으로 구성된 동적 시스템
  - 자동차, 항공, 군사 방어시스템 등의 모델링 및 시뮬레이션에 사용
- **ECML (ETRI CPS Modeling Language)**
  - 한국전자통신연구원에서 제안한 하이브리드 시스템 명세 언어
  - 모델링 및 시뮬레이션 기능 제공
  - Reachability analysis, 안전성분석을 위해 모델체킹을 추가로 적용할 필요가 있음

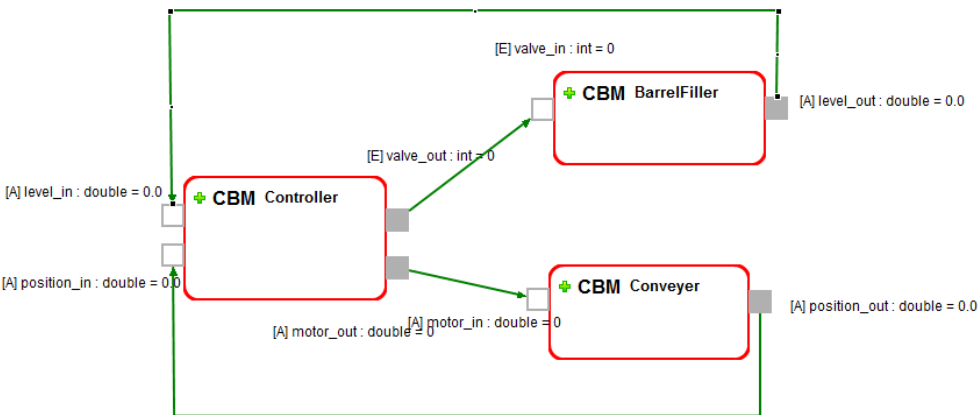
- ECML 모델의 모델체킹
  - 기존의 하이브리드 시스템 모델체커인 HyTech를 사용
- HyTech를 이용하기 위한 모델변환
  - ECML 모델을 선형하이브리드 오토마타로 변환
  - 변환된 선형하이브리드 오토마타를 HyTech 입력언어로 변환
- ECML 모델 체킹 결과의 분석
  - HyTech의 검증 결과는 기본적으로 GUI가 없음, 분석이 어려움
  - HyTechAnalyzer를 개발, 이를 이용한 분석
    - HyTech의 검증 결과를 시각화 해주는 도구

HyTech를 이용한 ECML 모델의 검증 및 분석

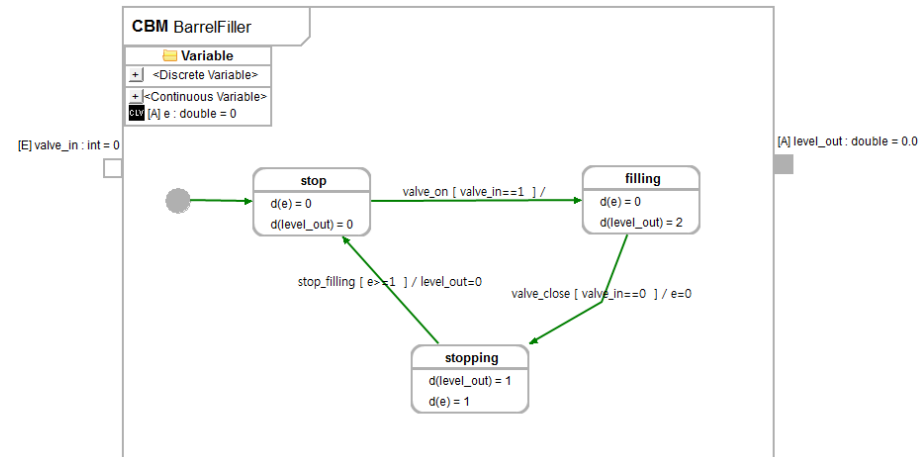
## 배경지식

# ECML (ETRI CPS Modeling Language)

- ECML의 구성
  - CBM : CPS Behavioral Model(행위모델)
  - CSM : CPS Structural Model(구조모델)
    - 하나 이상의 BM을 포함 할 수 있음 (Hierarchy)

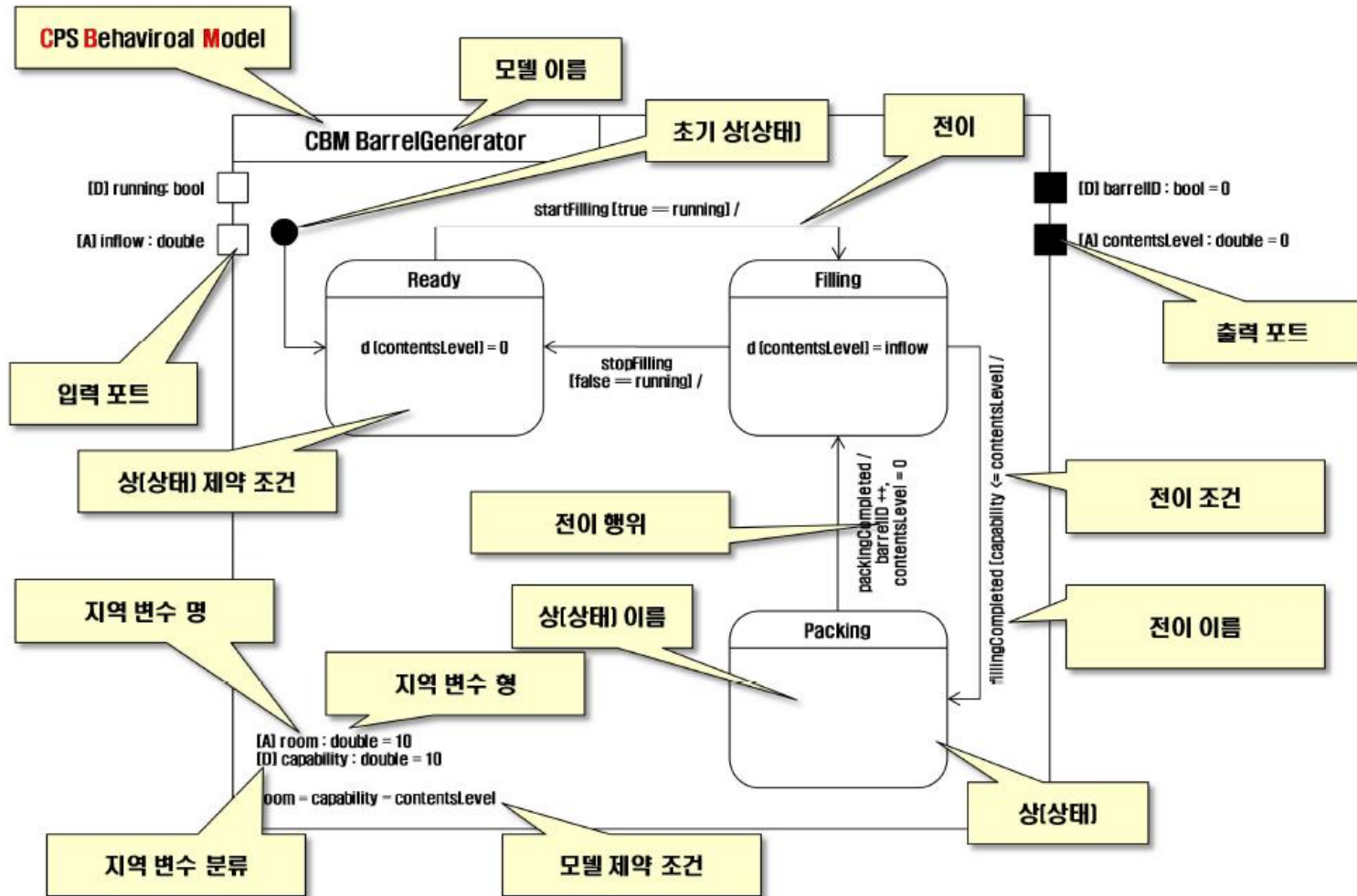


ECML 구조모델



ECML 행위모델

# CBM (CPS Behavioral Model)

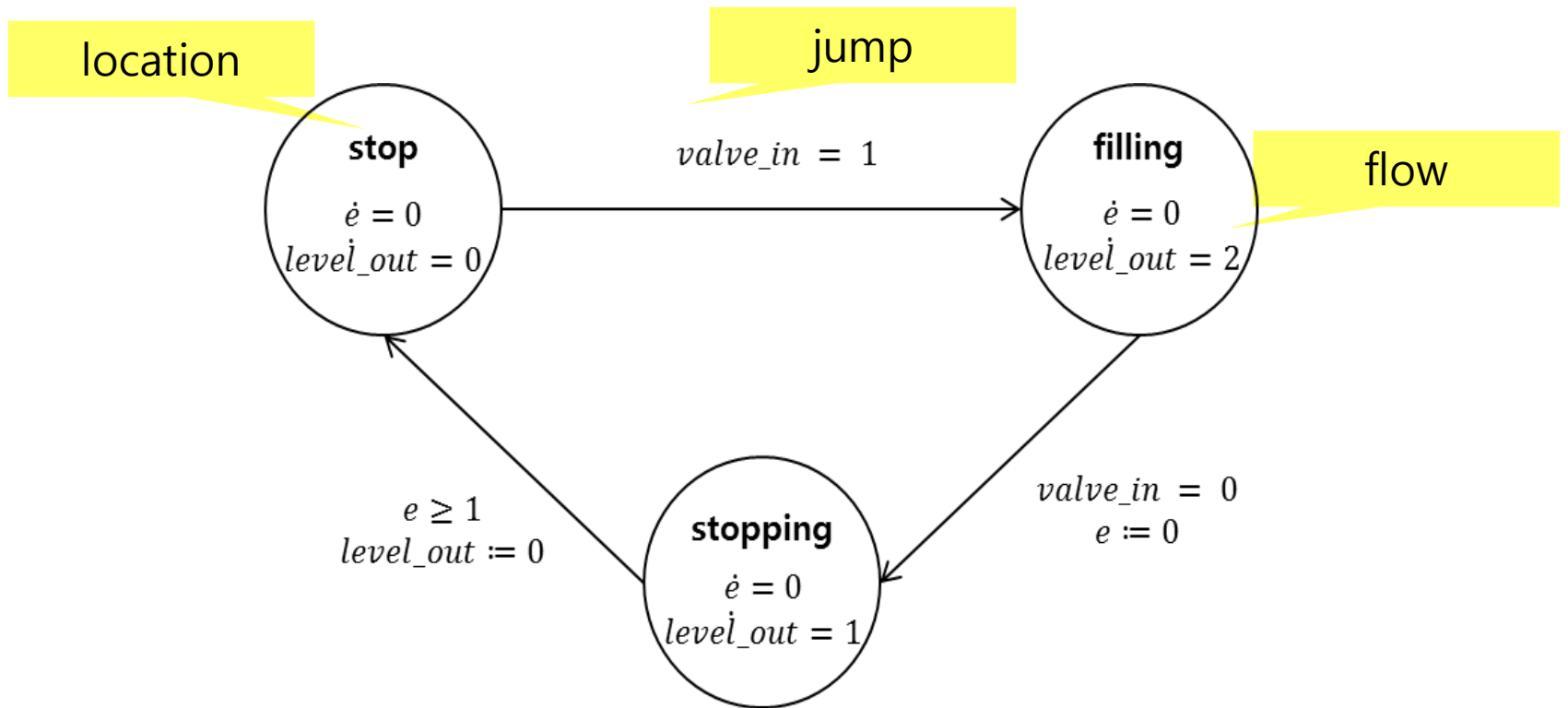


# HyTech와 선형하이브리드 오토마타

- HyTech
  - 하이브리드 시스템을 대상으로 하는 검증도구
  - 검증기능
    - Reachability
    - Parametric analysis
  
- 선형하이브리드 오토마타
  - HyTech 입력언어의 형태
  - 선형성(linearity) 제약 사항이 있는 하이브리드 오토마타
    - 연속 변수의 변화율은 상수
    - Invariant, initial condition은 1차식



# 선형 하이브리드 오토마타



# ECML 모델의 선형하이브리드 오토마타 변환

# 일대일 대응이 되는 부분

ECML

선형 하이브리드 오토마타

연속/이산 변수

연속/이산 변수

Invariant

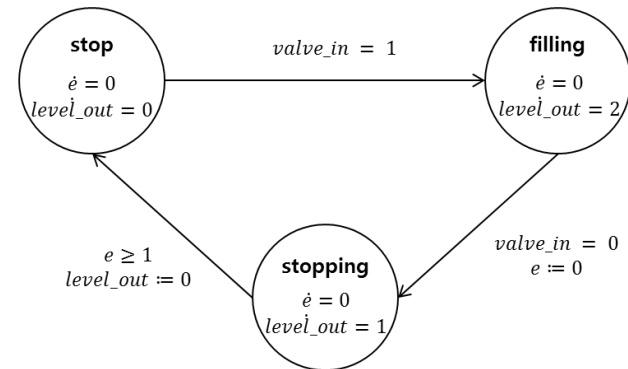
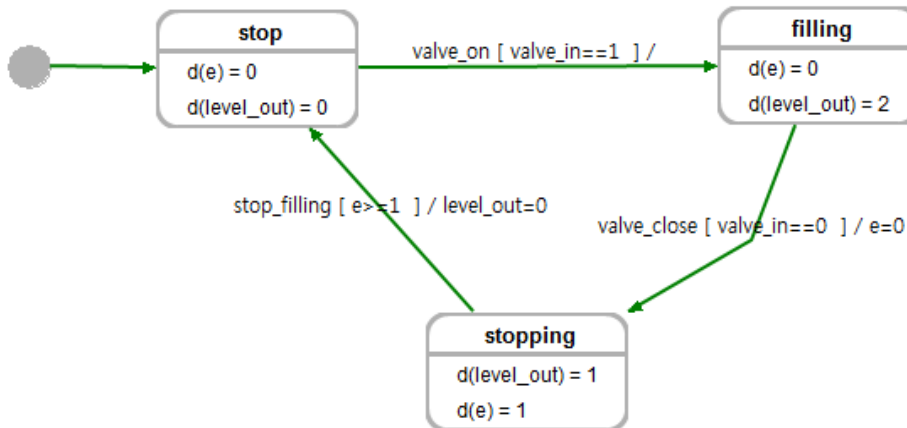
Invariant

Phase

Location

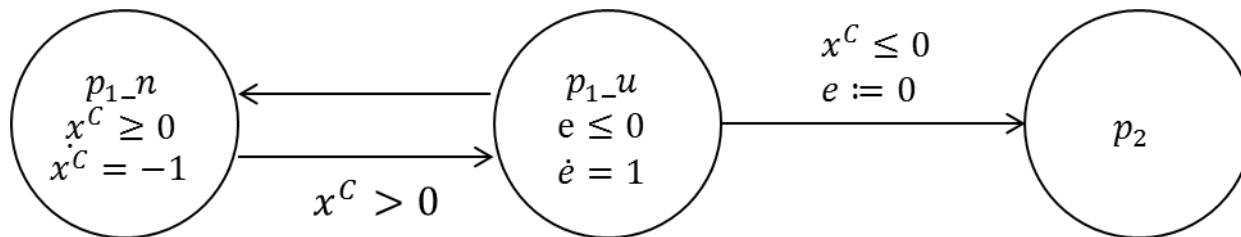
Rate

Flow



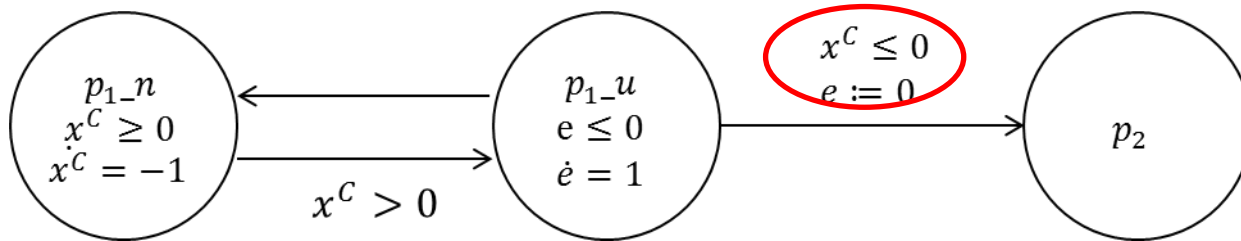
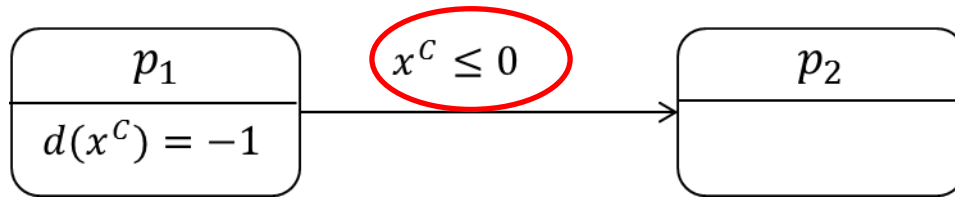
# 비결정적 전이

- ECML과 선형 하이브리드 오토마타의 전이의 특성이 다름
  - ECML은 결정적 전이 (deterministic)
  - 선형 하이브리드 오토마타는 비결정적 전이 (non-deterministic)
- Urgent location을 사용
  - $e$ 라는 변수를 추가, 변화율을 1로 invariant를  $e \leq 0$ 으로 하여 전이가 바로 발생하도록 함



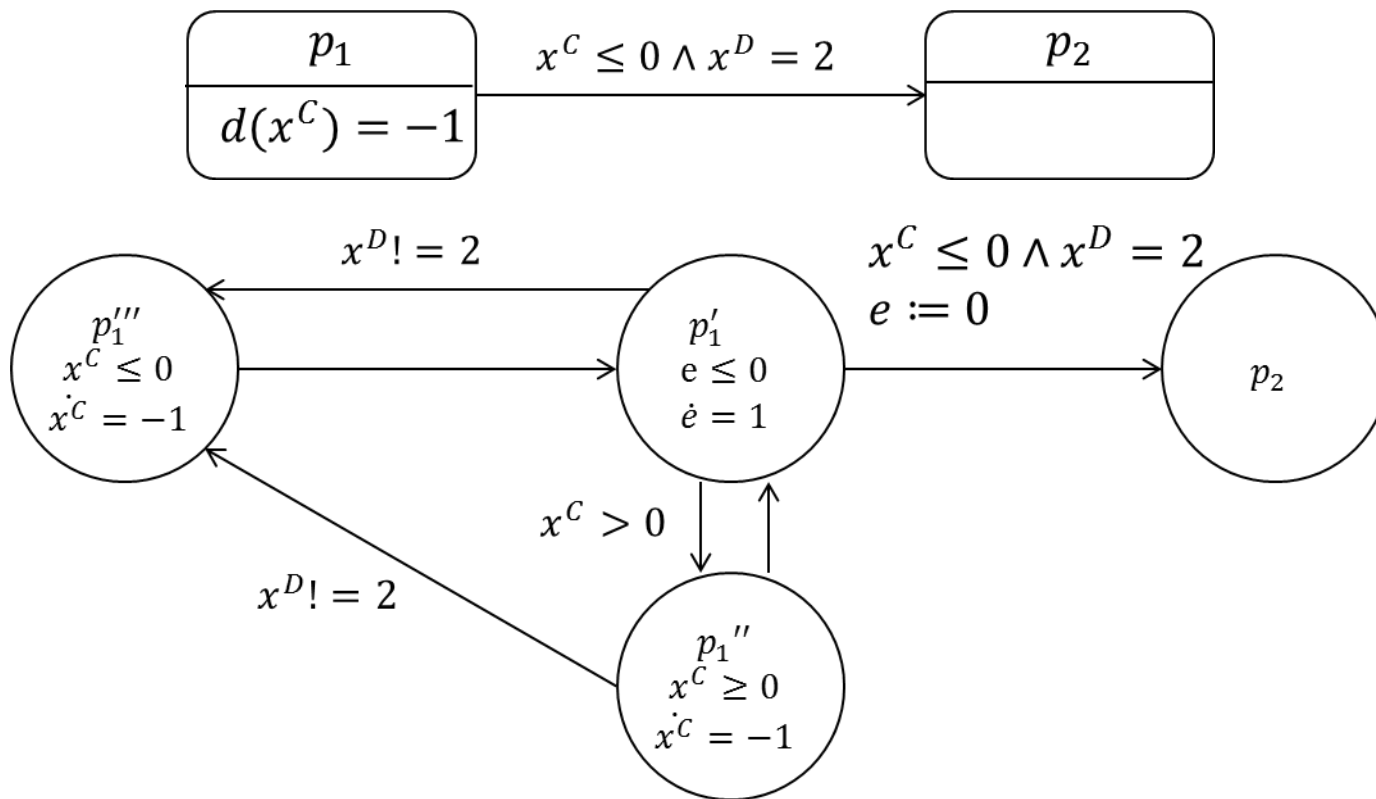
# 연속변수만 갖는 전이

- 전이의 조건을 갖는 jump와 전이의 조건의 역을 취한 jump로 변환



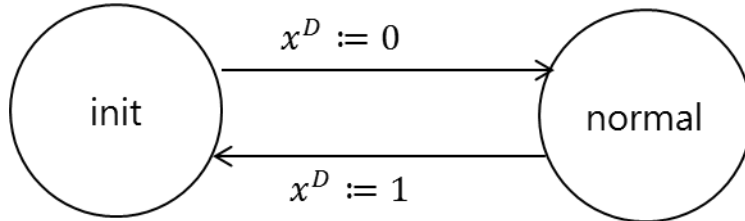
# 연속변수와 이산변수를 모두 갖는 전이

- 연속 변수와 이산 변수는 서로 독립적으로 값이 할당 될 수 있으므로 이를 고려한 변환이 필요

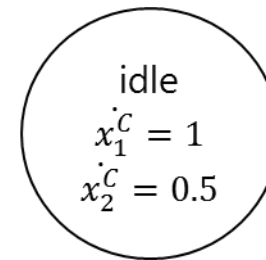


# 입력 오토마타

- 선형 하이브리드 오토마타에는 입출력 포트가 없으므로 이를 위한 입력 오토마타를 추가로 생성



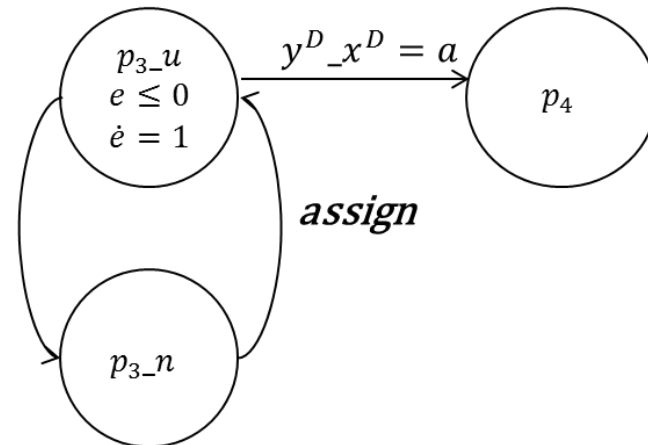
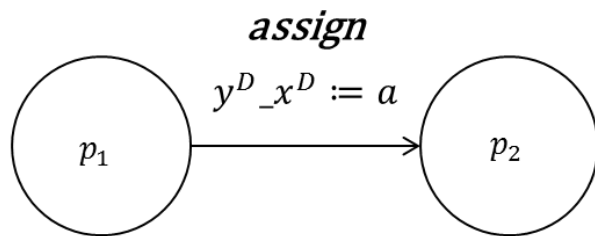
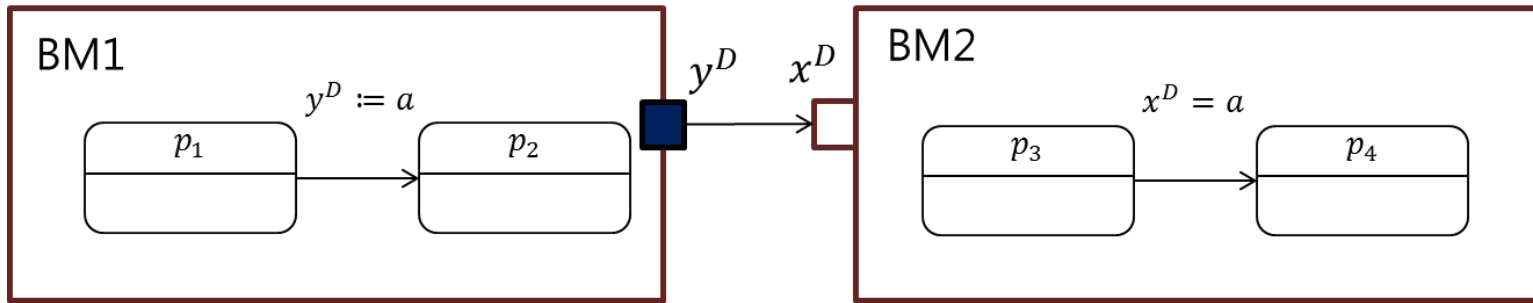
(a) 이산 변수에 대한 입력 오토마톤



(b) 연속 변수에 대한 입력 오토마톤

# 결합모델

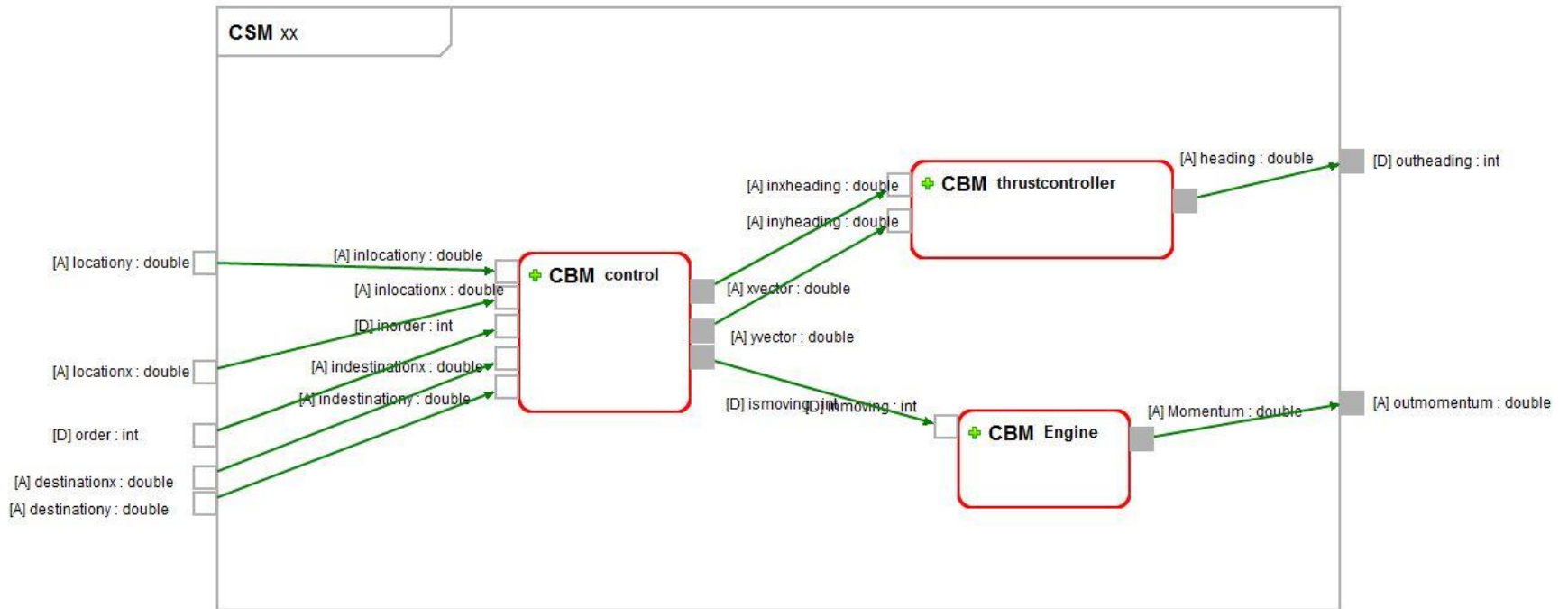
- 이산 변수의 특성을 고려, sync label을 사용 두 jump가 동시에 일어나게 함



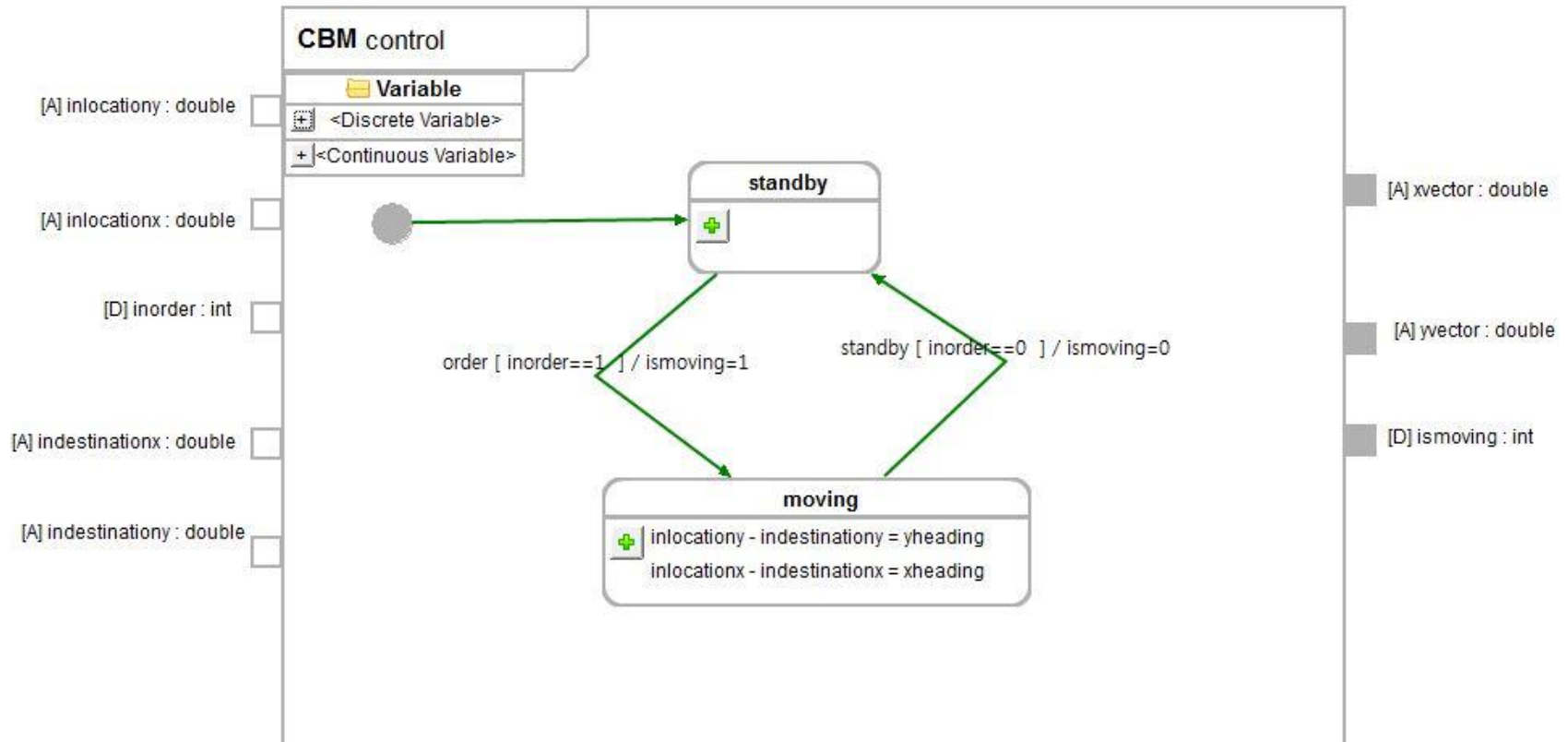


# 사례연구

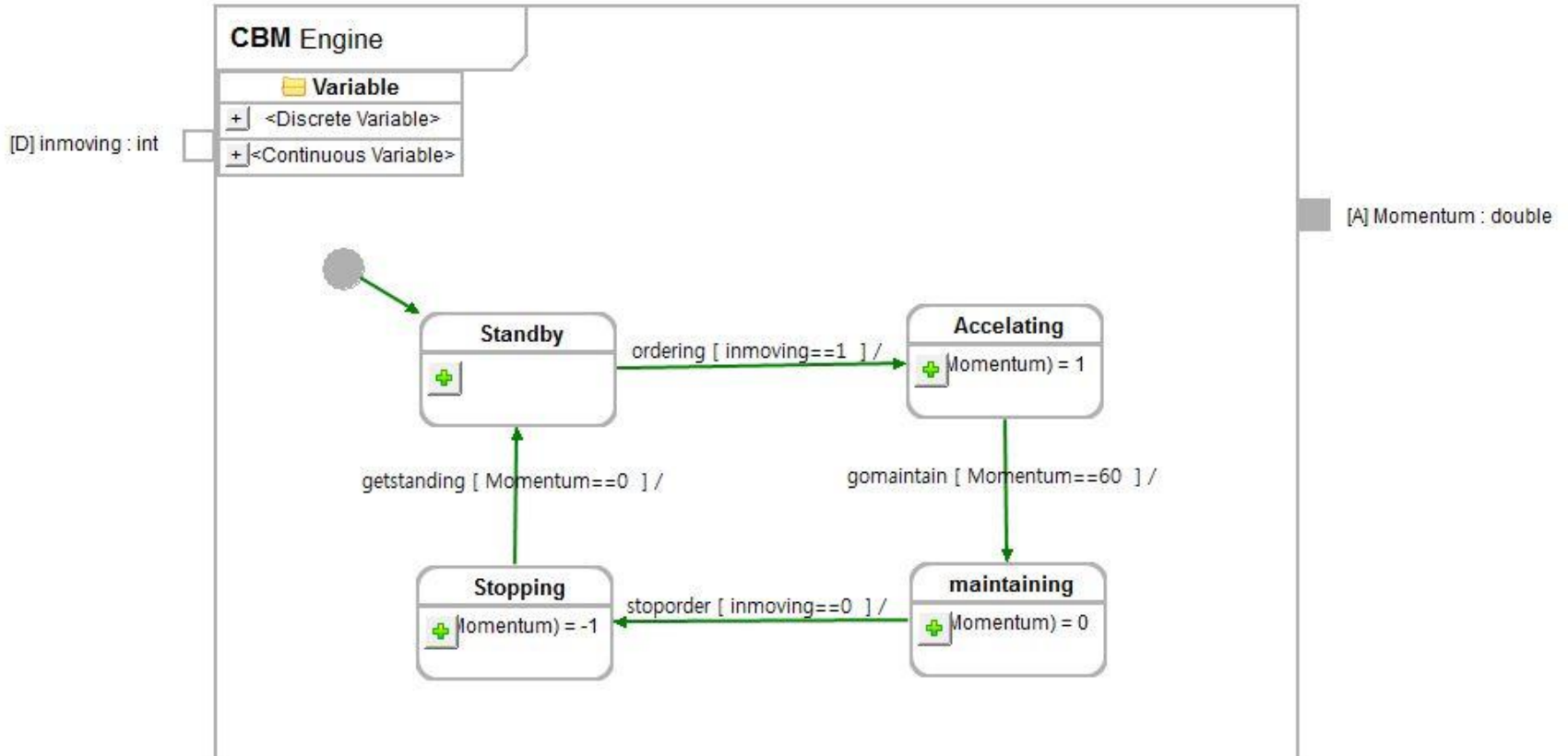
# 자동차 모델 – ECML 구조모델



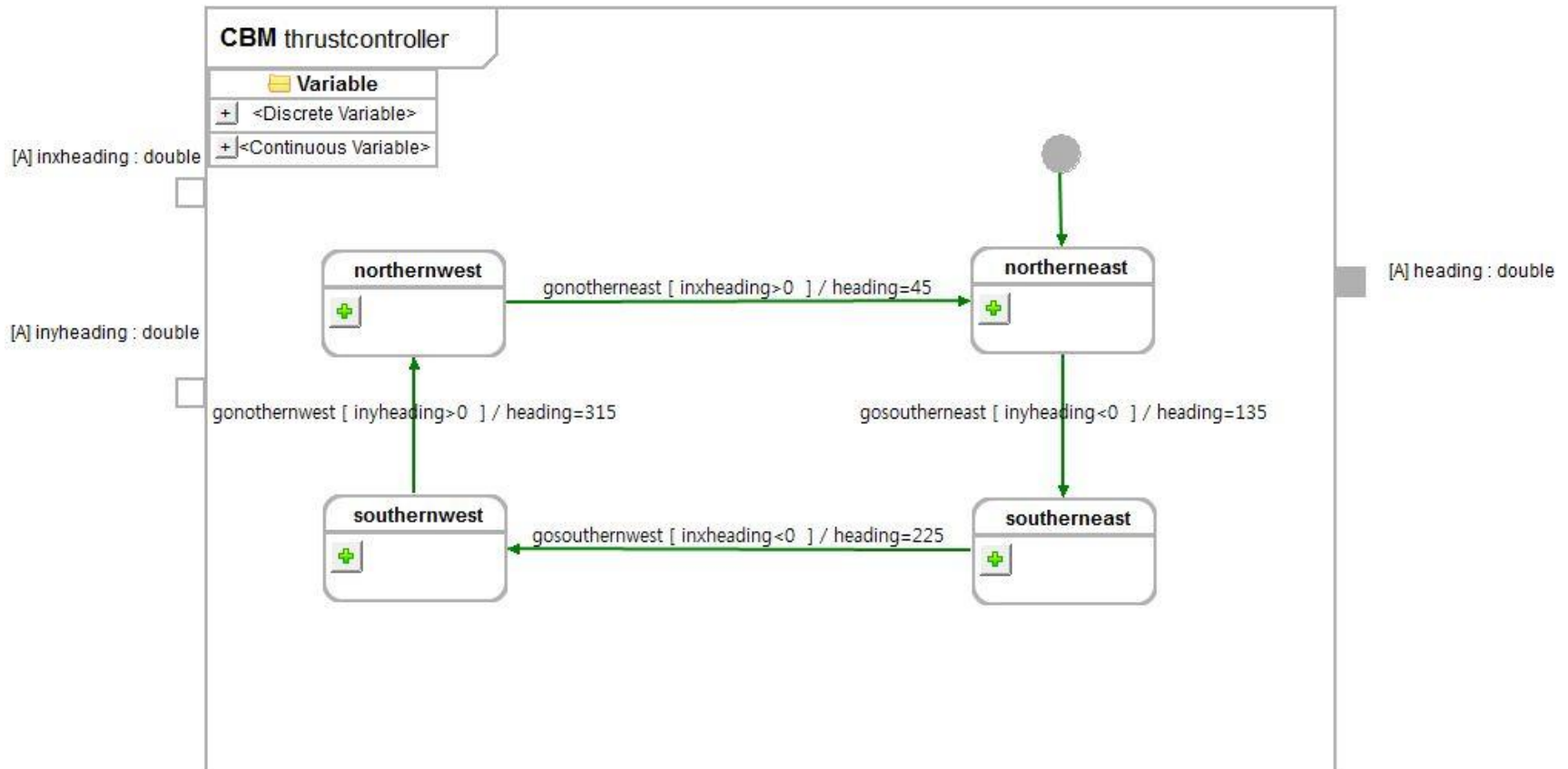
# ECML 행위모델 - controller



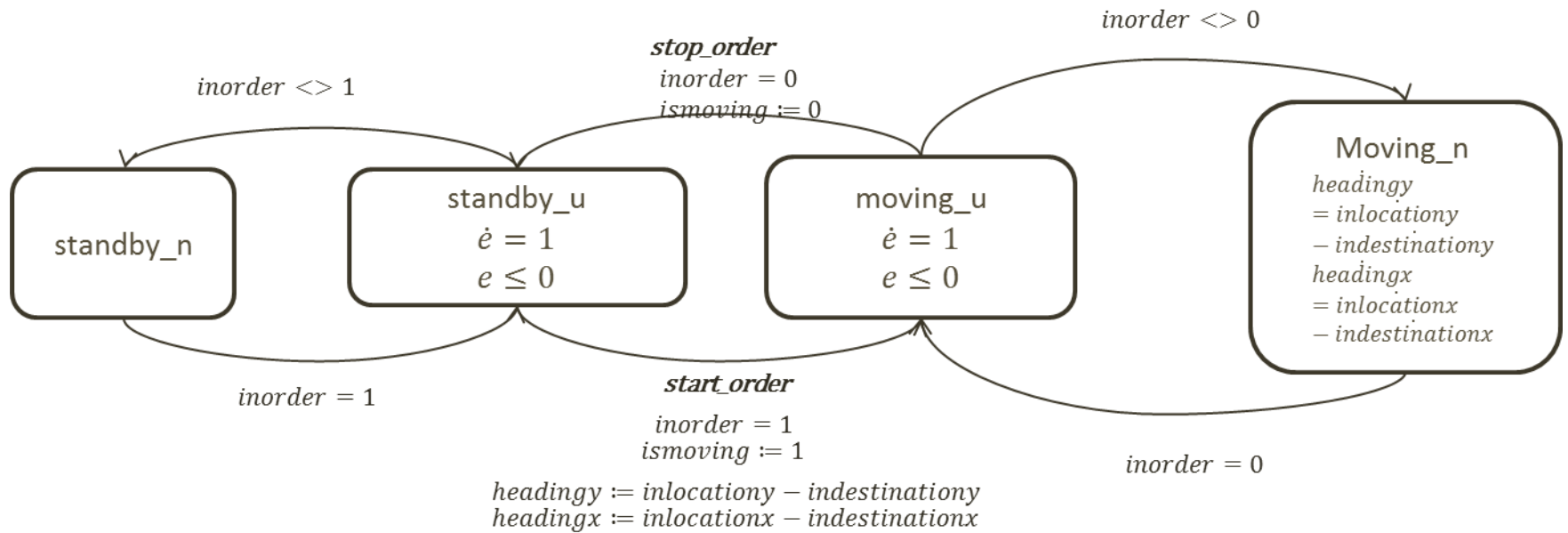
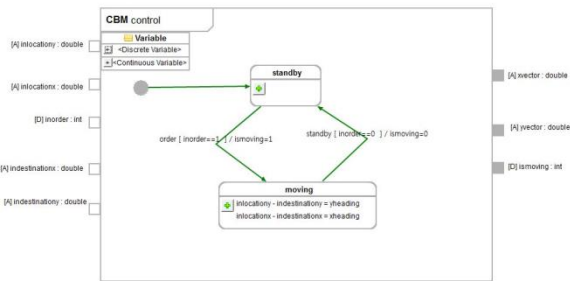
# ECML 행위모델- engine



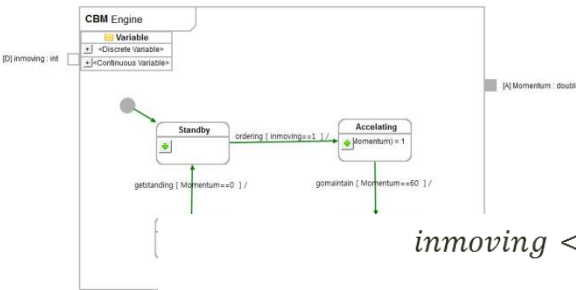
# ECML 행위모델- thrustcontroller



# 선형 하이브리드 오토마타 - controller

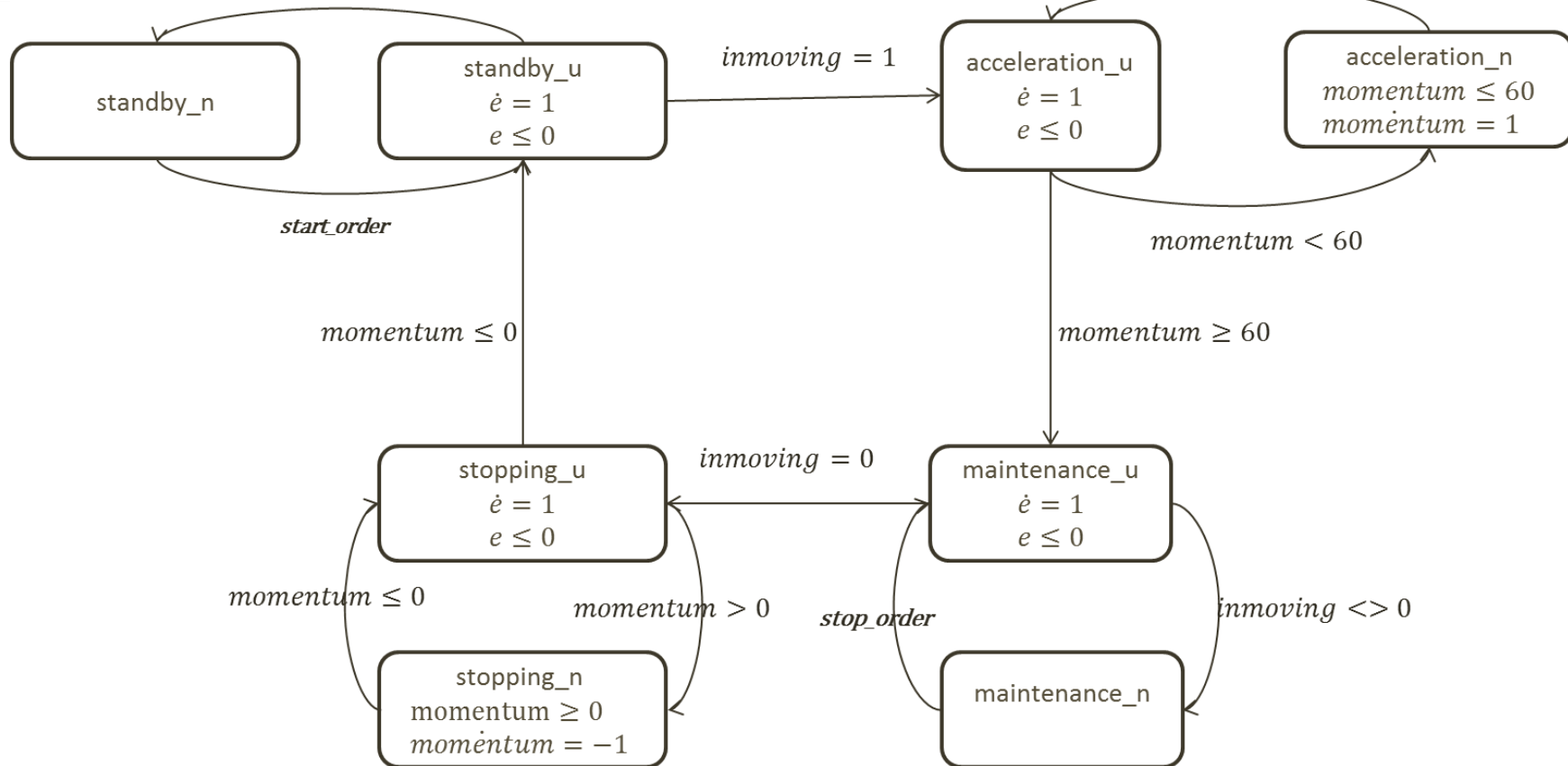


# 선형 하이브리드 오토마타 - engine

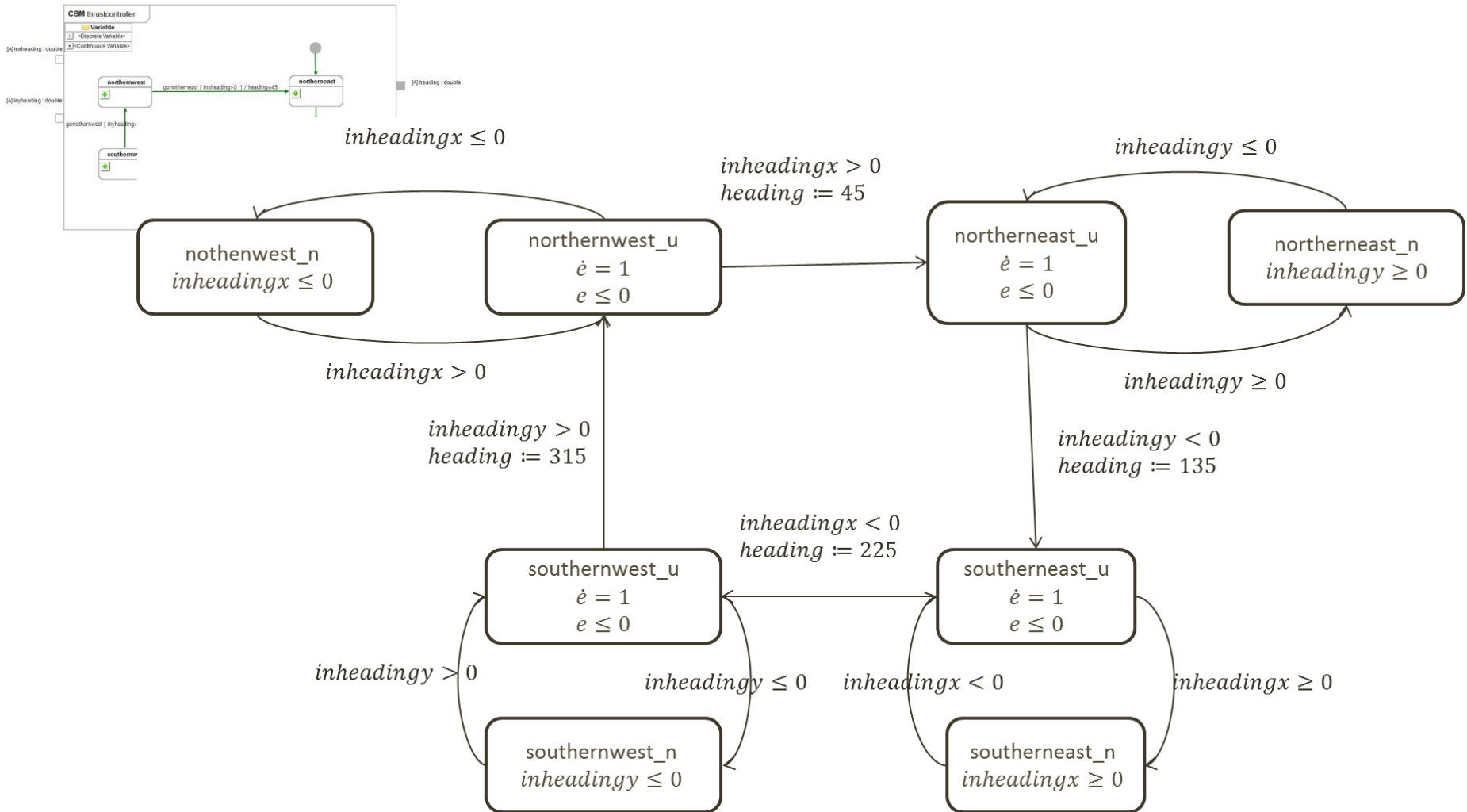


$inmoving \neq 1$

$momentum \geq 60$



# 선형 하이브리드 오토마타 - thrustcontroller

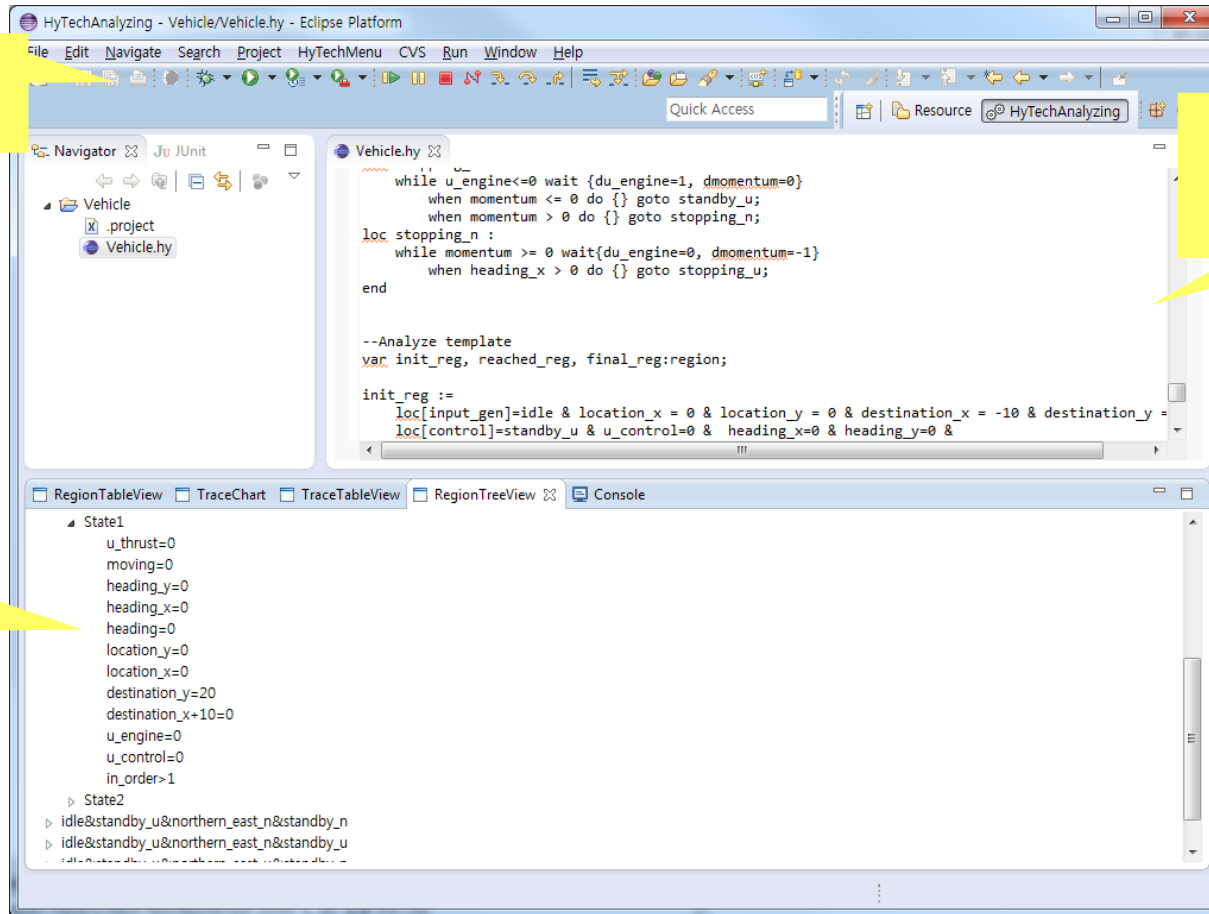




# HyTechAnalyzer

- HyTechAnalyzer를 이용한 HyTech 실행 및 분석

HyTech 실행



HyTech 코드  
편집

검증결과

# 검증결과

- 검증 속성
  - 자동차가 0°를 향하는 경우가 있는가?
  - 자동차가 처음 위치에서 목적지에 도착할 때까지 각 변수의 region (값의 범위)는 어떻게 되는가?
- 검증결과

Time	VIA	Automaton 1	Automaton 2	Automaton 3	Automaton 4	location_y	location_x	moving	u_control	in_order	destination_x	destination_y	momentum
0.0		idle	standby_u	northern_east_u	standby_u	0.0	0.0	0.0	0.0	0.0	-10.0	20.0	0.0

Automaton 1	Automaton 2	Automaton 3	Automaton 4	Status
idle	standby_n	northern_east_n	standby_n	u_thrust=0&moving=0&heading_y=0&heading_x=0&heading=0&location_y=0&location_x=0&destination_y=20&
idle	standby_n	northern_east_n	standby_n	u_thrust=0&moving=0&heading_y=0&heading_x=0&heading=0&location_y=0&location_x=0&destination_y=20&
idle	standby_n	northern_east_n	standby_u	u_thrust=0&moving=0&heading_y=0&heading_x=0&heading=0&location_y=0&location_x=0&destination_y=20&
idle	standby_n	northern_east_n	standby_u	u_thrust=0&moving=0&heading_y=0&heading_x=0&heading=0&location_y=0&location_x=0&destination_y=20&
idle	standby_n	northern_east_u	standby_n	u_thrust=0&moving=0&heading_y=0&heading_x=0&heading=0&location_y=0&location_x=0&destination_y=20&
idle	standby_n	northern_east_u	standby_n	u_thrust=0&moving=0&heading_y=0&heading_x=0&heading=0&location_y=0&location_x=0&destination_y=20&
idle	standby_n	northern_east_u	standby_u	u_thrust=0&moving=0&heading_y=0&heading_x=0&heading=0&location_y=0&location_x=0&destination_y=20&
idle	standby_n	northern_east_u	standby_u	u_thrust=0&moving=0&heading_y=0&heading_x=0&heading=0&location_y=0&location_x=0&destination_y=20&

# 결론

- ECML은 하이브리드 시스템을 위한 언어로 모델링 및 시뮬레이션을 지원
- ECML 모델을 safety/reachability analysis를 하기 위해 HyTech를 이용한 방법을 적용해보았음
- 현재의 방법은 선형성을 만족해야 한다는 제약사항이 있기 때문에 추가적인 방법이 필요