KU KONKUK UNIVERSITY

Translation from ECML to Linear Hybrid Automata

Jaeyeon Jo, Junbeom Yoo, Han Choi, Sungdeok Cha, Hae Young Lee and Won-Tae Kim

DEPENDABLE SOFTWARE LABORATORY

Contents

Introduction

- Hybrid System
  - Dynamical system – combination of continuous and discrete elements
  - Used in automotive controllers, avionic, and defense
- ECML
  - Modeling language for hybrid systems
  - An extension of the basic formalism DEV & DESS
  - Proposed by ETRI in Korea
- Formal Verification of ECML
  - Needs algorithmic method for verifying ECML

Introduction

- Hybrid Automata
  - Formal model for hybrid systems
- Linear Hybrid Automata(LHA)
  - Restricted Hybrid Automata using linear dynamics
    - If $\dot{a} = b$ and b is not constant, it is not linearity(x).
    - If $\dot{a} = b + c$ and b and c is constant, it is linearity(o).
- Related Study : Verification of DEV & DESS using HyTech
  - HyTech is model checking tool for linear hybrid automata
  - Translation from DEV & DESS into LHA

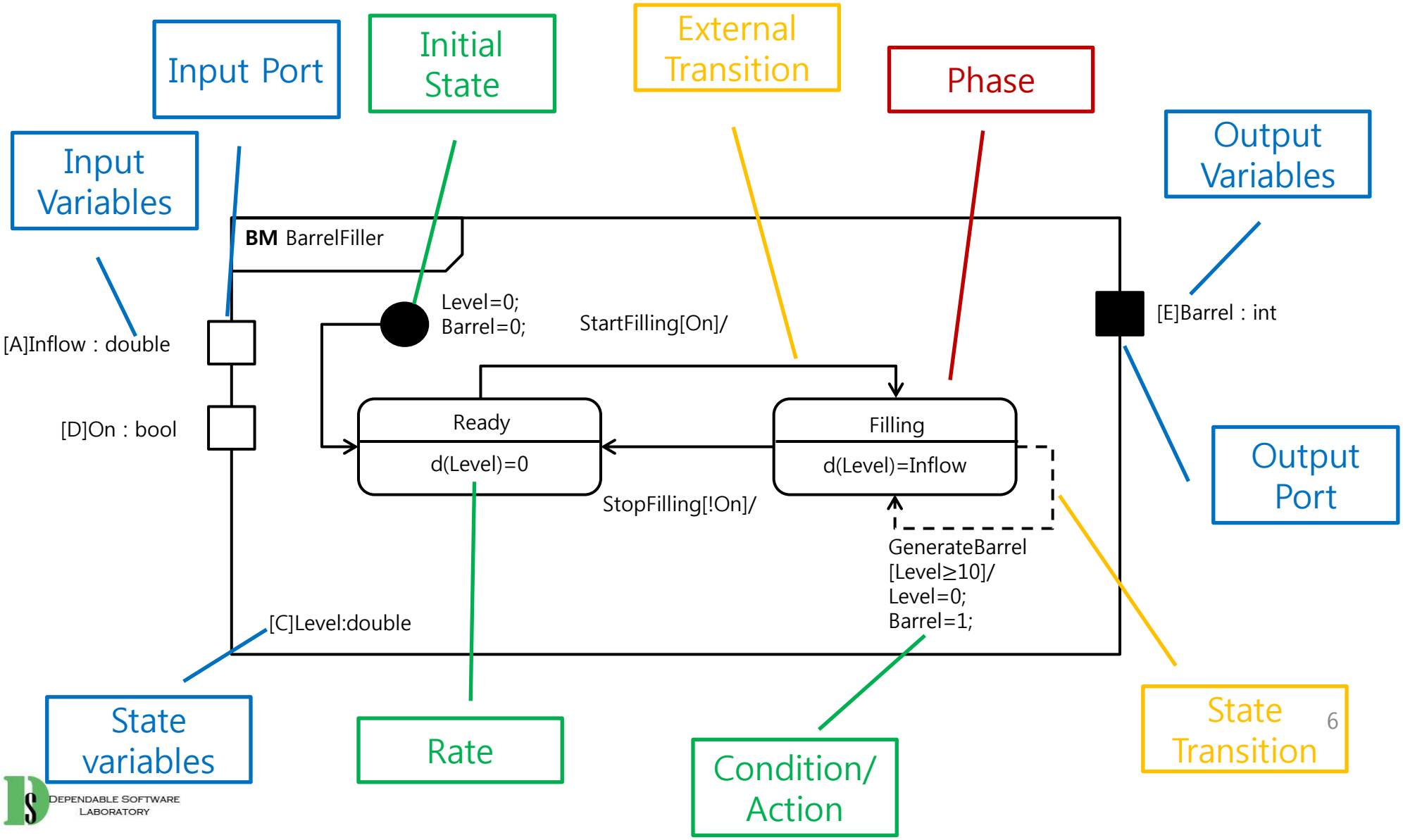
Introduction

- Translation rules from ECML into LHA
  - Semantics of ECML and LHA are different each other
  - Need to overcome semantic gap between ECML and LHA
  - HyTech verification on the ECML models.

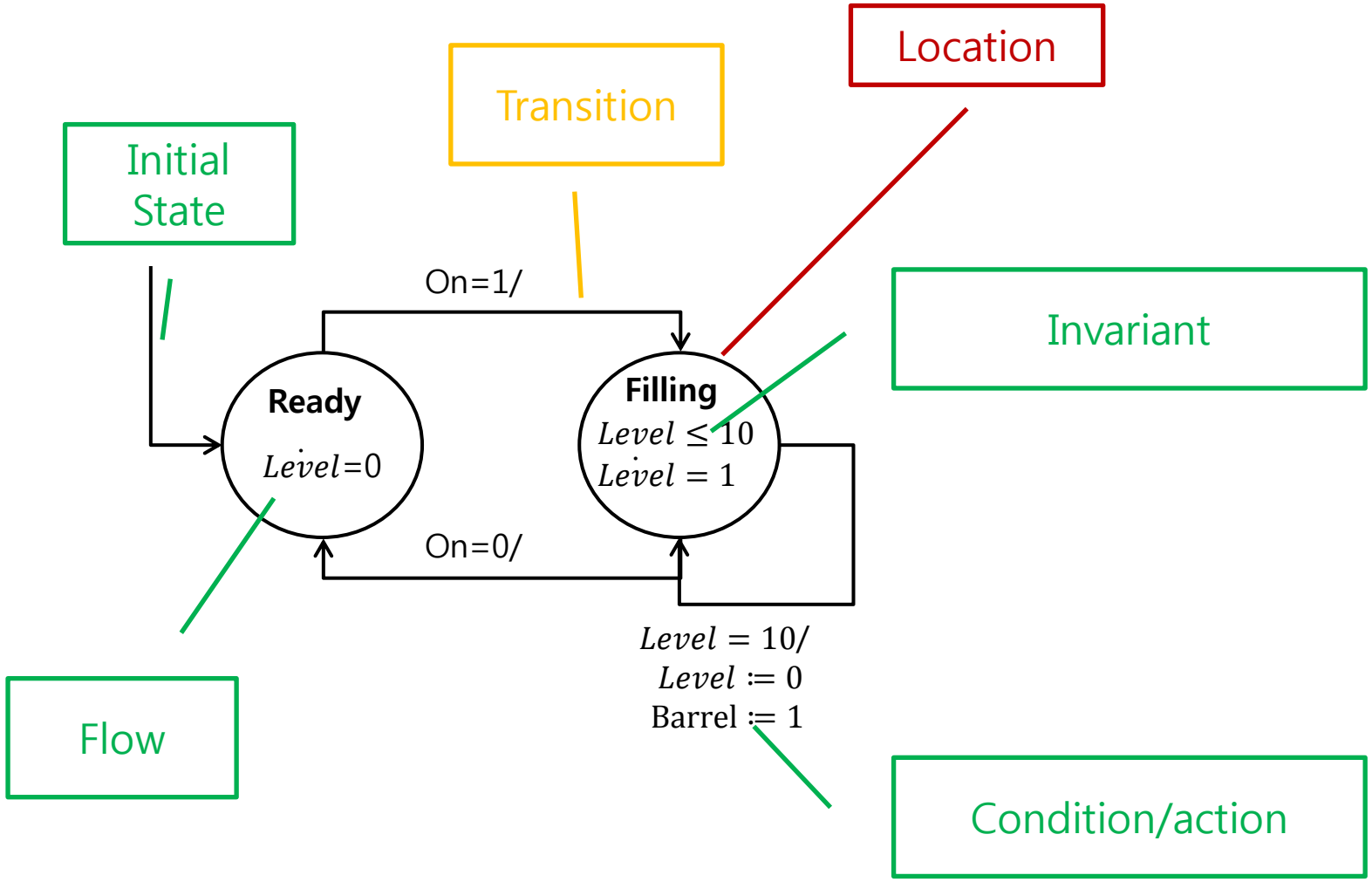
- Background
  - ECML
  - LHA

- ECML Model Translation
  - Single Model
  - Coupled Model

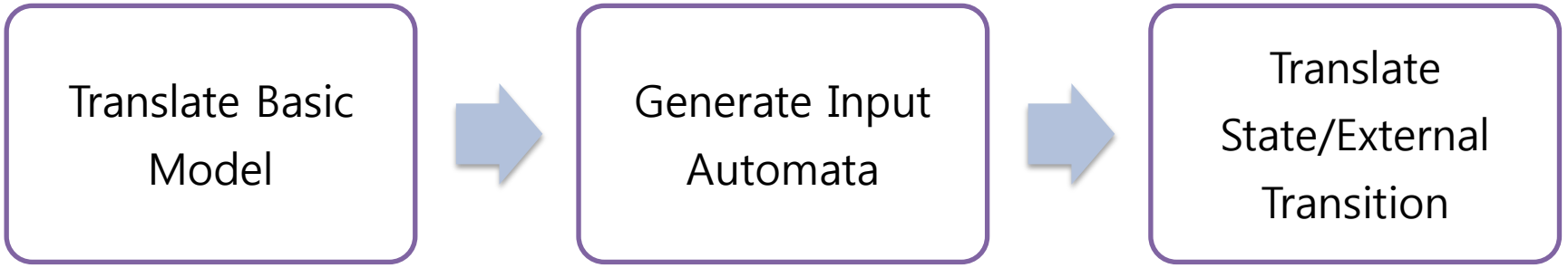
ECML Basic Model



Linear Hybrid Automata

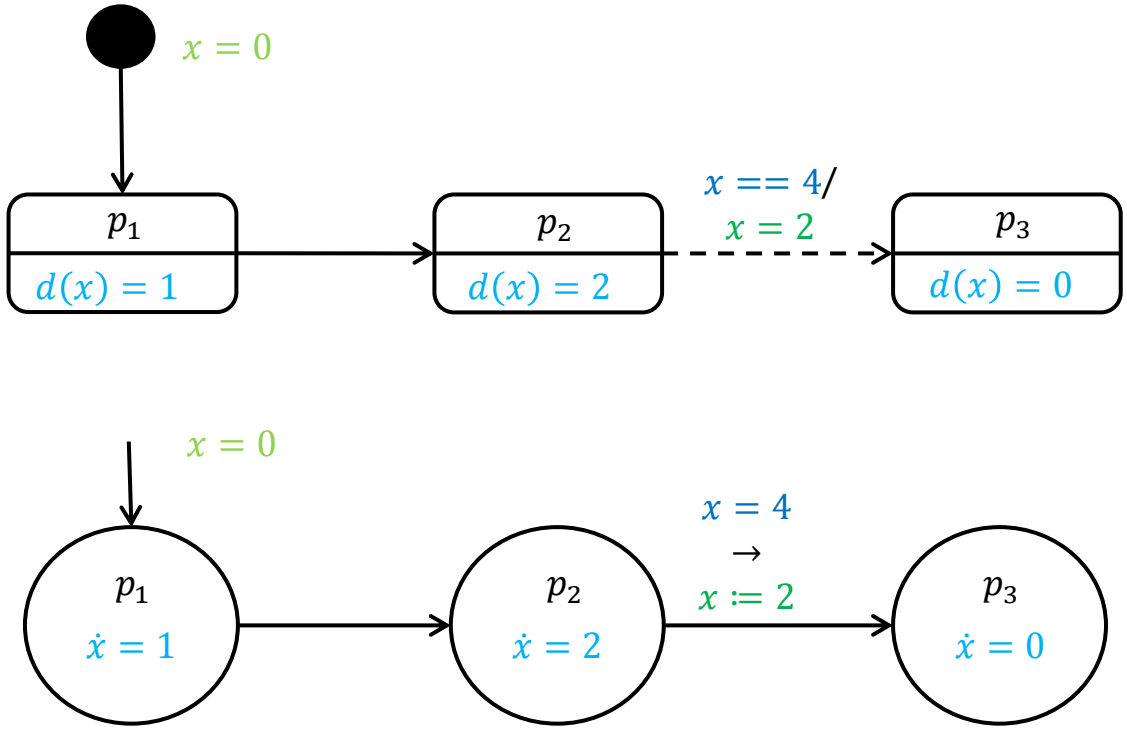


ECML Model Translation Process



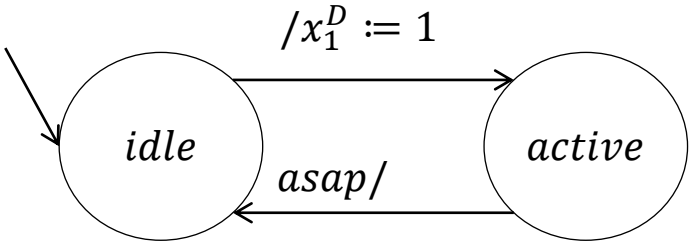
Basic Model Translation

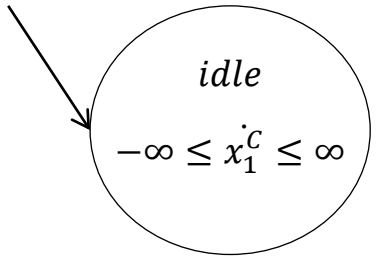
- We first translate the models without type of transition
  - All of element should coincide with each other.



Generate Input Automata

- Generate discrete input automata
  - Discrete input automaton is controlling discrete input variables of ECML
- Generate continuous input automata
  - Continuous input automaton is controlling continuous input variables of ECML
  - Continuous input could be changed continuously

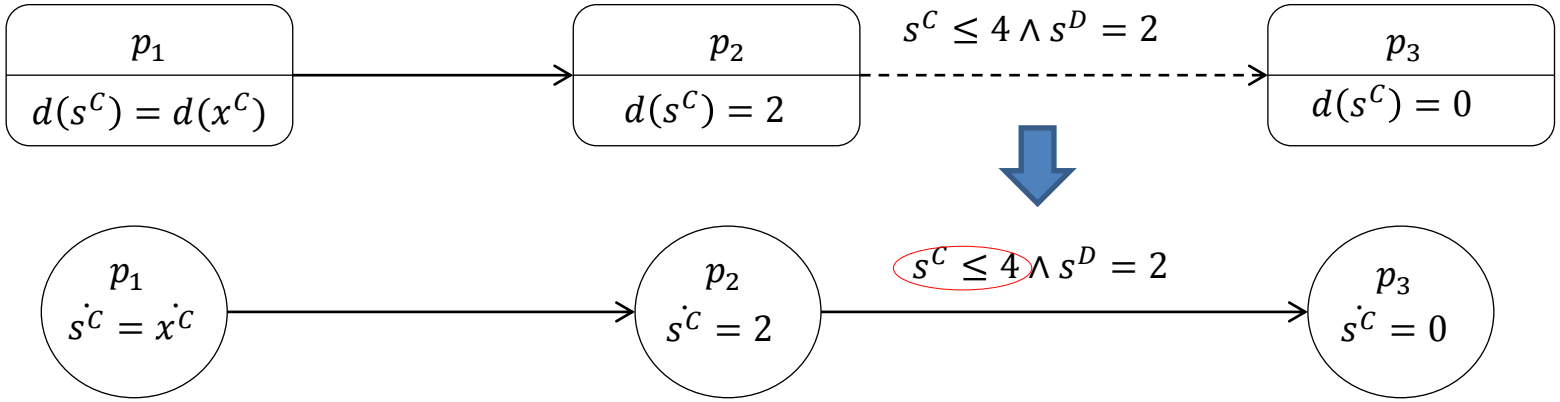




State Transition

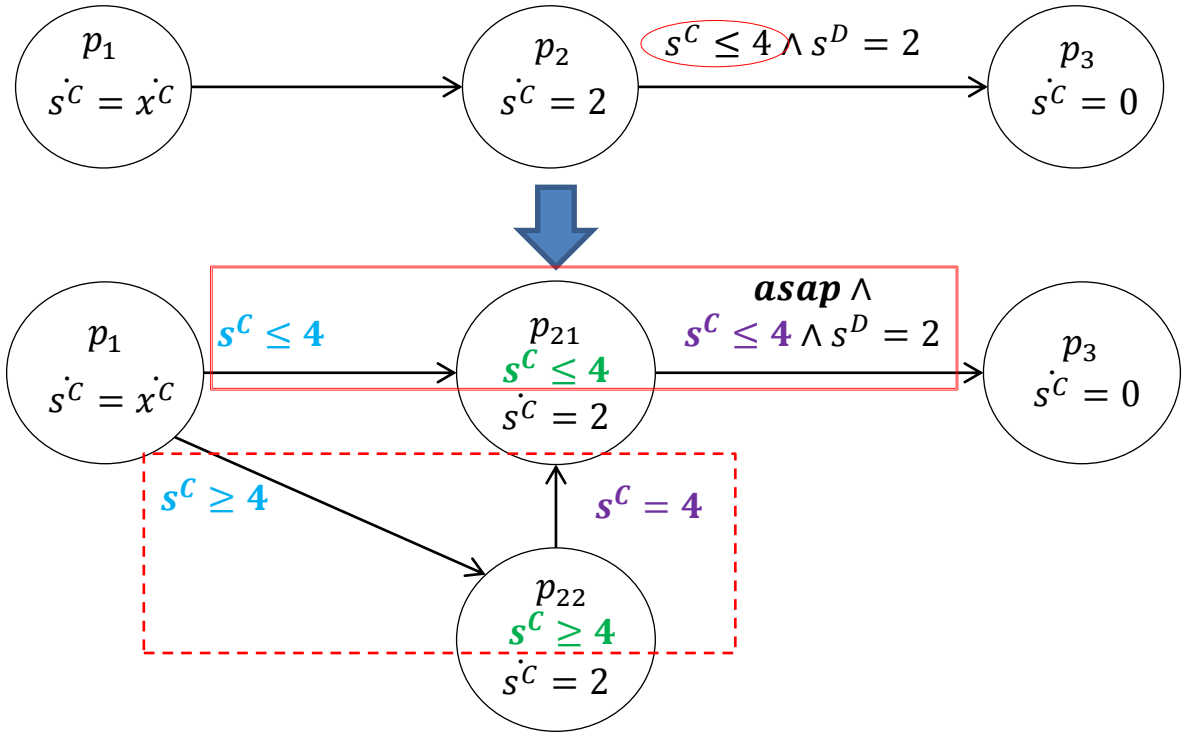
- A condition for the state transitions are defined as
  - $C=(\varphi_1{}^C \wedge \varphi_2{}^C \wedge \ldots \wedge \varphi_n{}^C \wedge \varphi_1{}^D \wedge \varphi_2{}^D \wedge \ldots \wedge \varphi_m{}^D)$
    - φ^C is an atomic proposition for continuous terms
      - ex) $s^c \leq x^D$
    - φ^D is an atomic proposition for discrete terms
      - ex) $x^D \leq 1$

- Only φ^C is considered in the state transition translation.



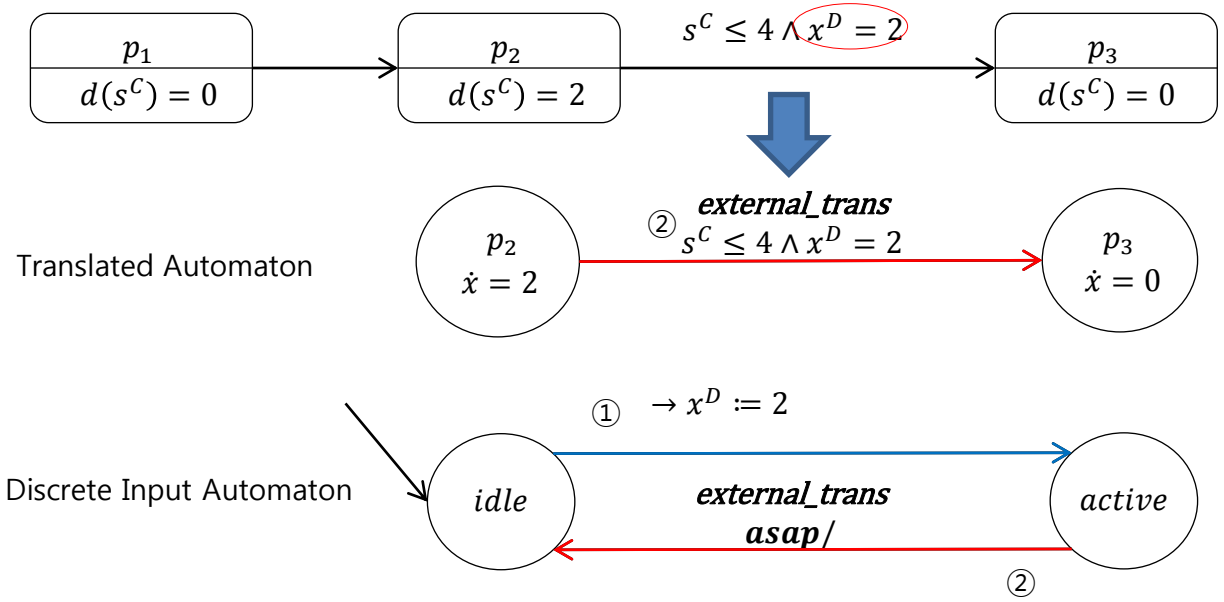
State Transition

φ^C	z=z′			z<z′			z≤z′		
item	$Cond_{prev}$	Invariant	$Cond_{out}$	$Cond_{prev}$	Invariant	$Cond_{out}$	$Cond_{prev}$	Invariant	$Cond_{out}$
Current	z=z′	z=z′	z=z′	z<z′	z≤z′	z≤z′	z≤z′	z≤z′	z≤z′
Negation	z<z′	z≤z′	z=z′	z≥z′	z≥z′	z=z′	z>z′	z≥z′	z=z′
	z>z′	z≥z′	z=z′						



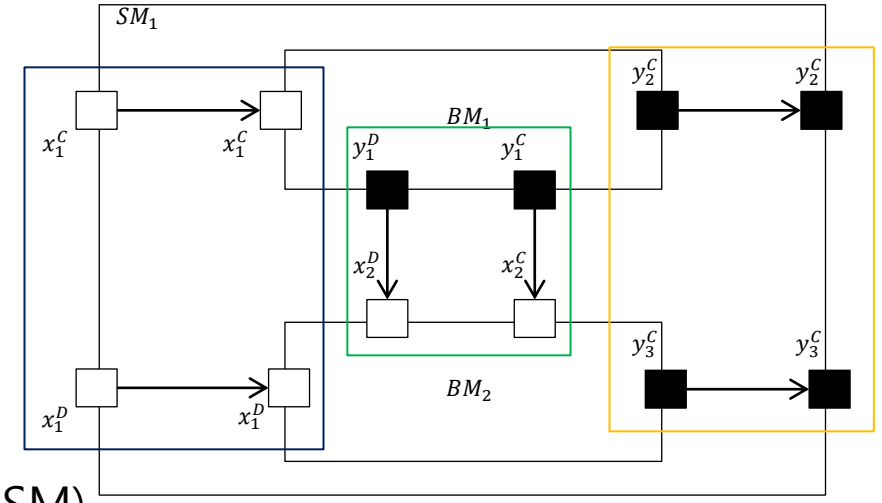
External Transition

- External transition translation
  - Generate a transition in discrete automaton to determine the time of executing external transition
  - Add a synchronization label to the transition in discrete automaton and external transition

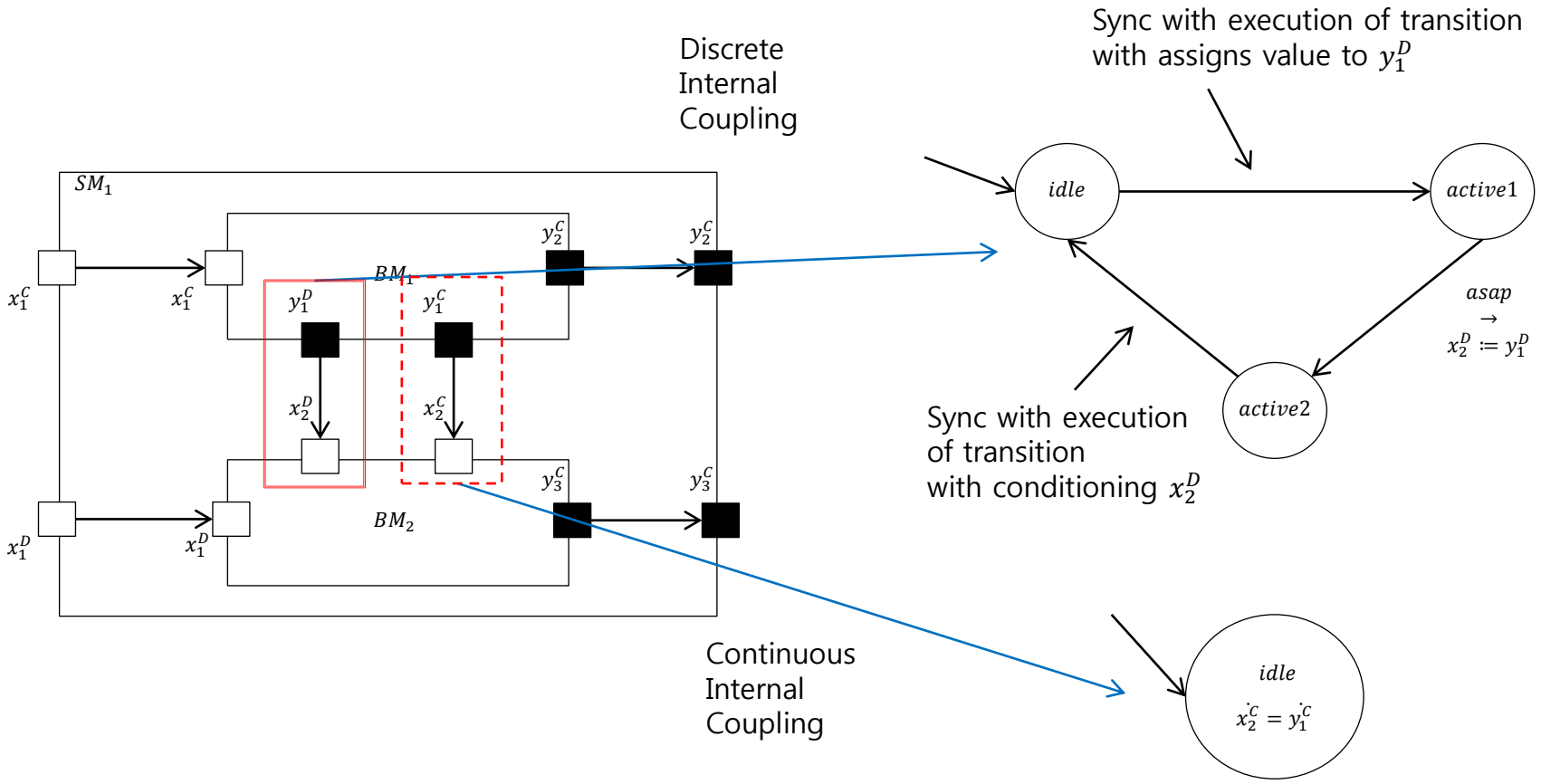


ECML Structural Model

- Structured model is coupled model for ECML
- ECML structural model(SM) contains basic model(BM)s or SM which connects each other
- Input coupling
  - Input port(SM) -> Input port(BM)
- Output coupling
  - Output port(BM) -> Output port(SM)
- Internal coupling
  - Output port(BM, BM) -> Input port(BM, SM)



Internal Coupling Translation



Conclusion

- Hybrid system
  - Hybrid system has composed discrete elements and continuous elements
  - Hybrid automata and ECML are modeling language for hybrid system
- Our work
  - Propose a translation rule from ECML into LHA to verify ECML model
  - Developed a translation tool ECML to LHA
- Future work
  - Verify ECML model using hybrid system verification tools such as SpaceEx, PHAVer.

Q & A