Case study : ECML Verification Using SpaceEx

Jaeyeon Jo, Sanghyun Yoon, Jumbeom Yoo, Hae Young Lee, Won-Tae Kim

KonKuk Univ, ETRI

DEPENDABLE SOFTWARE LABORATORY

Contents

1. Introduction
2. Background
    1. ECML
    2. Hybrid Automata
3. Verification of Barrel-filler Model
    1. ECML model of Barrel-filler
    2. Verification of barrel-filler system
4. Conclusion

Hybrid System

- Hybrid system
  - Models combination of continuous elements and discrete elements
  - Used in automotive, medical, and avionic systems
  - Linear hybrid automata
    - $ax + b = 0$, a and b are constants

- Hybrid system verification tools
  - Reachability Analysis – HyTech, PHAVer, SpaceEx
  - Deductive Proving – KeyMaera, HSolver

- ECML
  - Hybrid System Modeling Language
  - Extends DEV & DESS
  - ETRI proposed it to develop a cyber physical system

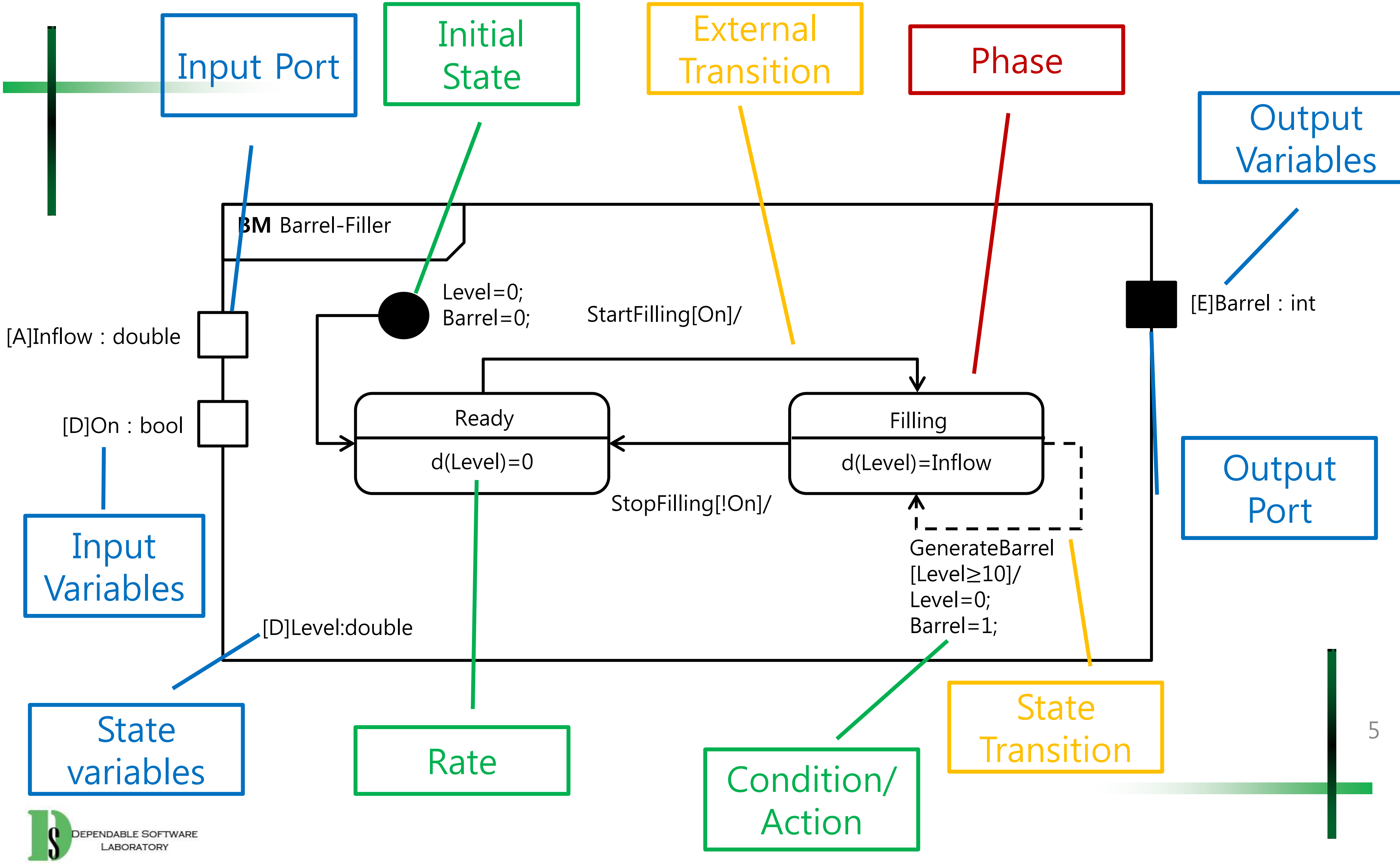
ECML Verification Using SpaceEx

- Previous studies
  - ECML and DEV & DESS are translated into linear hybrid automata for verification using HyTech
  - ECML and DEV & DESS restricted by linearity

- SpaceEx
  - A tool framework for non-linear hybrid automata
  - Contains PHAVer which verifies linear hybrid automata

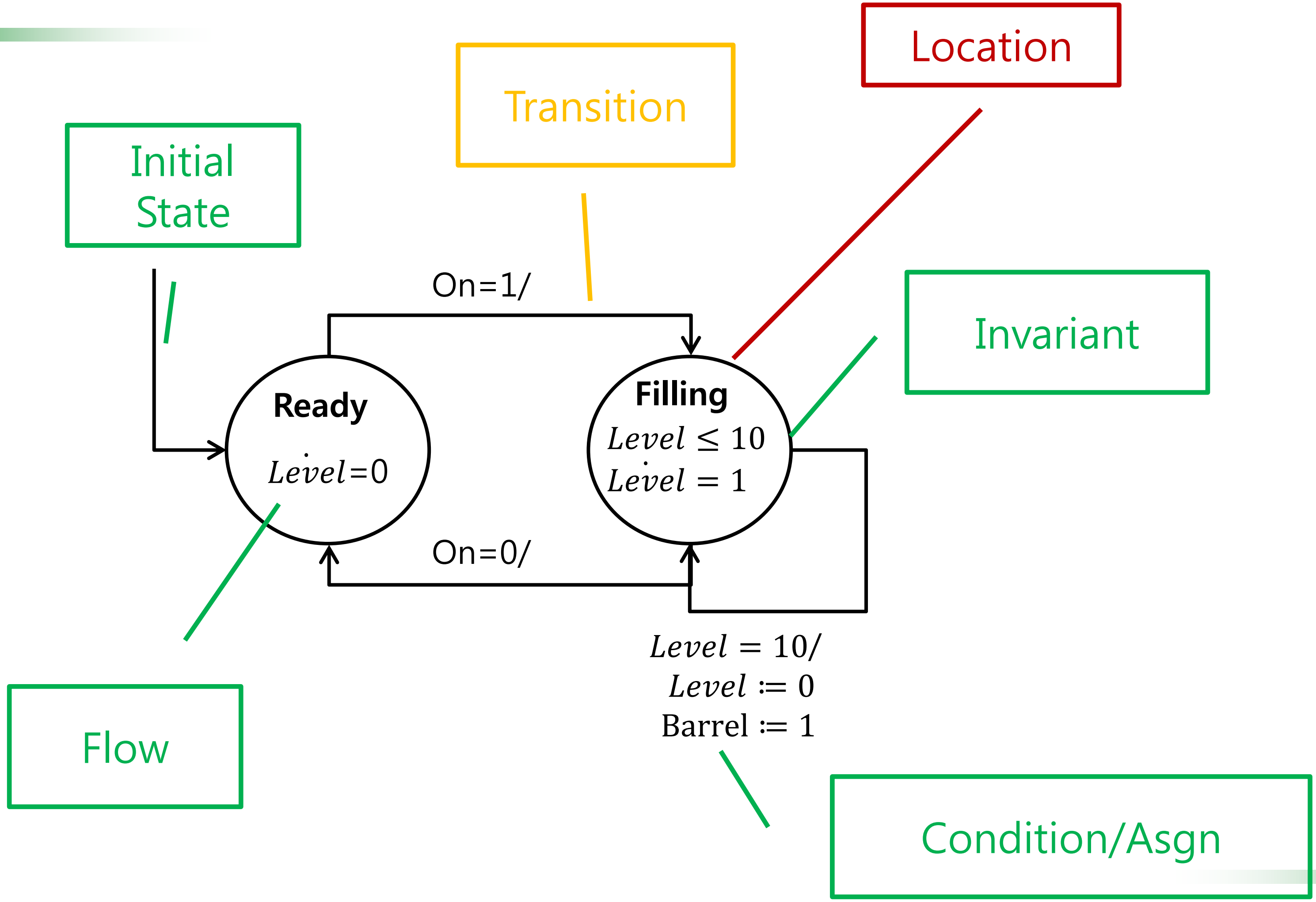
- ECML Verification Using SpaceEx
  - Using translation from ECML into Hybrid Automata
  - Extends scope of verifiable ECML model
  - Models Barrel-filler system to show translation

ECML



Input Port
Initial State
External Transition
Phase
Output Variables
BM Barrel-Filler
Level=0;
Barrel=0;
StartFilling[On]/
[E]Barrel : int
[A]Inflow : double
[D]On : bool
Ready
d(Level)=0
Filling
d(Level)=Inflow
StopFilling[!On]/
Output Port
Input Variables
GenerateBarrel
[Level≥10]/
Level=0;
Barrel=1;
[D]Level:double
State variables
Rate
Condition/ Action
State Transition

Hybrid Automata



Hybrid Automata of SpaceEx

- SpaceEx contains PHAVer

- PHAVer verifies hybrid automata that consists of linear dynamics or hybrid automata with affine dynamics
  - $Flow(l)$ is a continuous dynamics of the form $A\dot{x}(t) + b_0 \bowtie 0$
  - $Asgn$ is of the form $x' \bowtie Ax + b_0$
  - $\bowtie \in \{<, \leq, =\}$ is an operator

- SpaceEx verifies non-linear hybrid automata
  - $Flow(l)$ is a continuous dynamics of the form $\dot{x}(t) = Ax(t) + Bu(t) + b_0$, $u(t) \in U$
  - $Asgn$ is of the form $x' = Ax + Bu + b_0$
  - U is nondeterministic input set

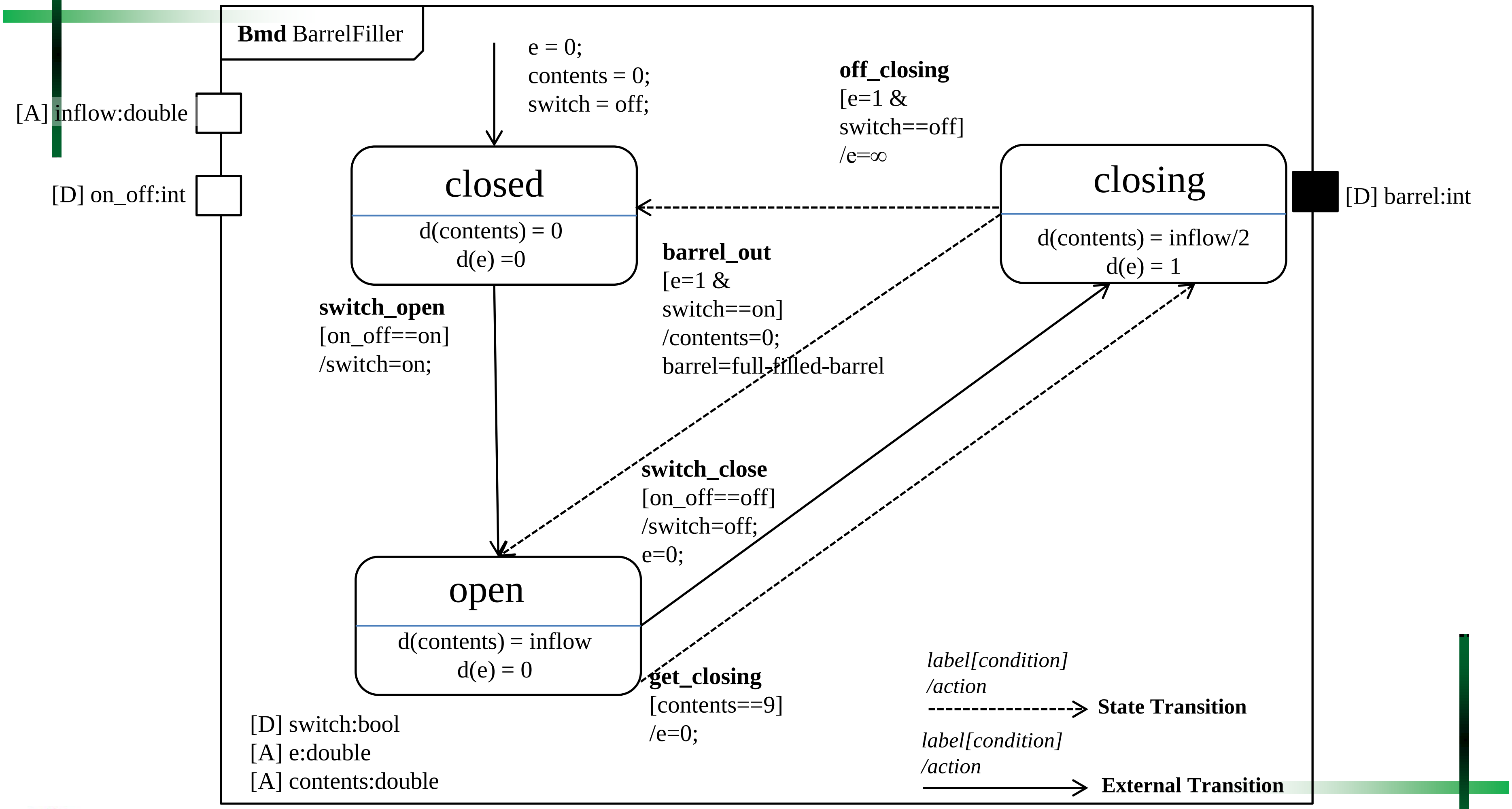
Semantic Difference of Two Language

- Input/output
  - ECML has input/output port structure
  - Hybrid automata have no input/output structure
- Type of transition
  - ECML has external transition and state transition those are executed when condition is satisfied
  - Hybrid Automata has transitions those are depend on invariant condition
- Coupling
  - ECML have coupling structure using connecting ports
  - Hybrid Automata uses synchronization label

Barrel-filler System Specification

- System description
  - Barrel-filler system fills a barrel with a specific inflow rate
  - Puts the barrel whenever the barrel is filled up to specific water level(10)
- Components
  - $\boldsymbol{on\_off}$ input determines starting or stopping filling barrels
  - $\boldsymbol{switch}$ have state of on or off
  - $\boldsymbol{Inflow}$ is input water flow to barrel
  - $\boldsymbol{barrel}$ contains water
  - $\boldsymbol{contents}$ is the level of water in barrel
  - $\boldsymbol{full-filled-barrel}$ is a signal about when a barrel is filled to a specific level
- Valve States
  - open – inflow rate is 1 to 2
  - closing – inflow rate is 1 and waits 1 time unit
  - closed – inflow rate is 0

Barrel-filler - ECML



Bmd BarrelFiller

[A] inflow:double

[D] on_off:int

[D] barrel:int

e = 0;
contents = 0;
switch = off;

closed
d(contents) = 0
d(e) =0

closing
d(contents) = inflow/2
d(e) = 1

open
d(contents) = inflow
d(e) = 0

off_closing
[e=1 &
switch==off]
/e=∞

barrel_out
[e=1 &
switch==on]
/contents=0;
barrel=full-filled-barrel

switch_open
[on_off==on]
/switch=on;

switch_close
[on_off==off]
/switch=off;
e=0;

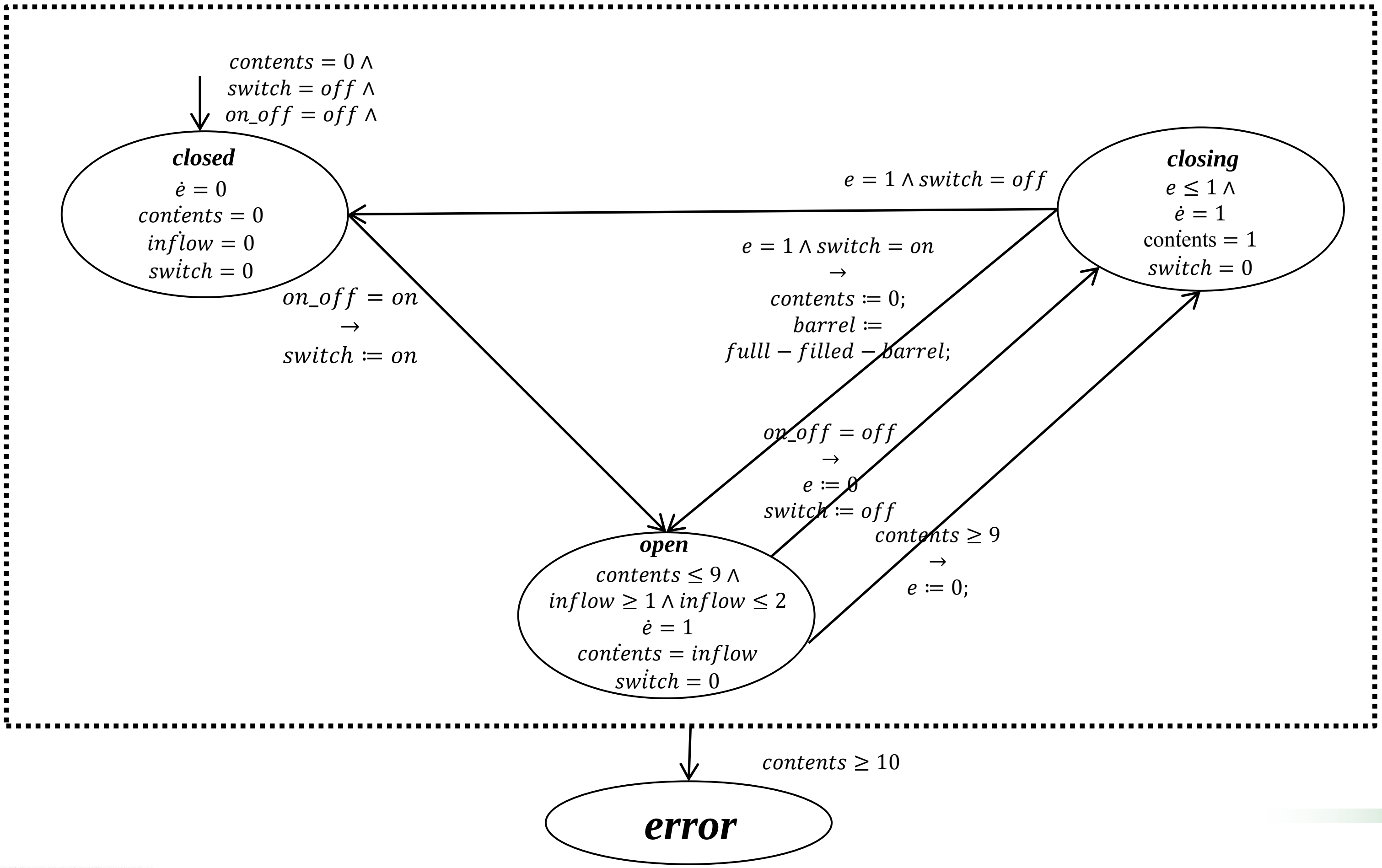
get_closing
[contents==9]
/e=0;

[D] switch:bool
[A] e:double
[A] contents:double

label[condition]
/action
State Transition

label[condition]
/action
External Transition

Barrel-filler Model - Hybrid Automata



Trajectory of Barrel-filler System

- Trajectory of barrel-filler system
  - shows same behavior of ECML model and LHA

- Point of time
  - **T0** - The valve is closed and the barrel is empty
  - **T1** - Filling is initiated by the discrete input signal on
  - **T2** – Input signal off and filling is stopped
  - **T5** – Filling starts again by input signal on
  - **T8~9** – closing valve and contents is about to 10

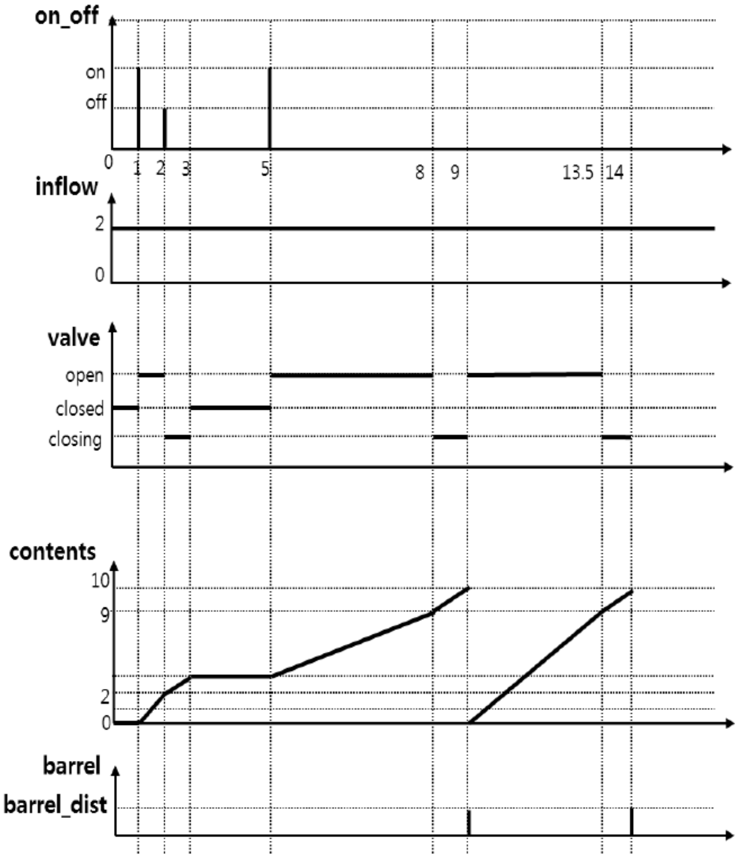
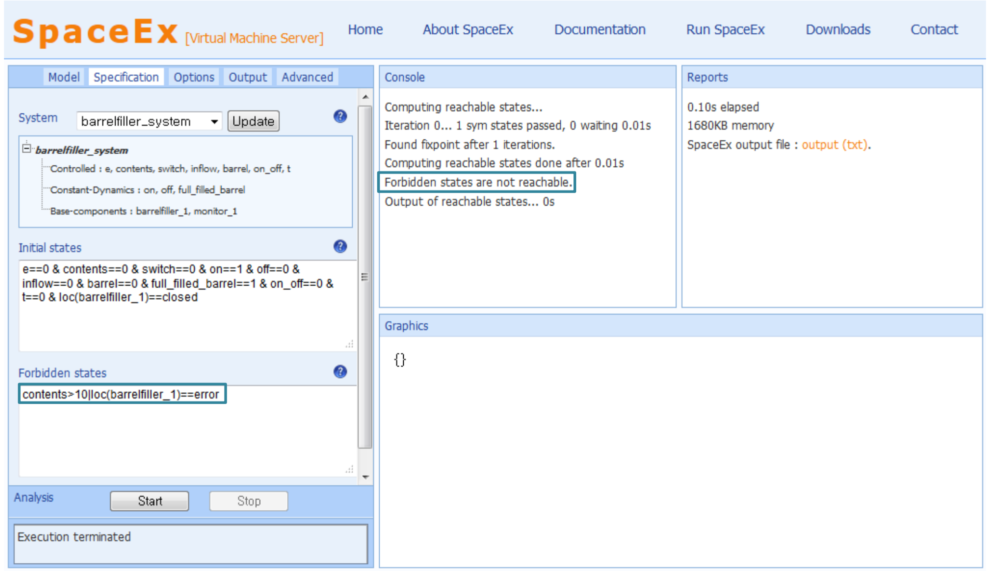


Fig. 2 A behavior of barrel-filler model

Safety Property

- Safety Property of Barrel-filler system
  - Property : Contents must not exceeds 10 and system cannot be error state
  - Forbidden states : $contents > 10 \lor loc(barrelfiller) = error$
    - $contents > 10$: Contents is a level of barrel, It must not exeeds 10
    - $loc(barrelfiller) = error$: Barrel system control modes not in error states
  - Result : Forbidden state are not reachable – satisfy safety property



System barrelfiller_system

barrelfiller_system
- Controlled : e, contents, switch, inflow, barrel, on_off, t
- Constant-Dynamics : on, off, full_filled_barrel
- Base-components : barrelfiller_1, monitor_1

Initial states

```
e==0 & contents==0 & switch==0 & on==1 & off==0 &
inflow==0 & barrel==0 & full_filled_barrel==1 & on_off==0 &
t==0 & loc(barrelfiller_1)==closed
```

Forbidden states

```
contents>10|loc(barrelfiller_1)==error
```

```
Execution terminated
```

Console

```
Computing reachable states...
Iteration 0... 1 sym states passed, 0 waiting 0.01s
Found fixpoint after 1 iterations.
Computing reachable states done after 0.01s
Forbidden states are not reachable.
Output of reachable states... 0s
```

Reports

```
0.10s elapsed
1680KB memory
SpaceEx output file : output (txt).
```

Graphics

```
{}
```

Conclusion

- Background
  - ECML is a modeling language for hybrid system, but verification tool is not developed yet
  - SpaceEx is a reachability analysis tool for hybrid automata

- Contribution
  - Proposed a translating approach for formal verifications of ECML models using hybrid automata as an example of barrel-filler system

- Limitation & Future works
  - An ECML model with non-linear dynamics has not been verified yet
  - Try to verify ECML model as non-linear hybrid automata using SpaceEx

Q & A