南京大學
NANJING UNIVERSITY

Online Hybrid Automata Verification of Dynamical Cyber-Physical System

Lei Bu
Nanjing University
bulei@nju.edu.cn

Joint Work with Qixin Wang and Xuandong Li

September 20th， Clarke Symposium 2014

- Congratulation to Ed!
- I was a visiting student in Ed’s group Sep 07-Sep 08
- Great Mentor, I learned a lot from here
- E.g. Cyber-Physical System

Outline

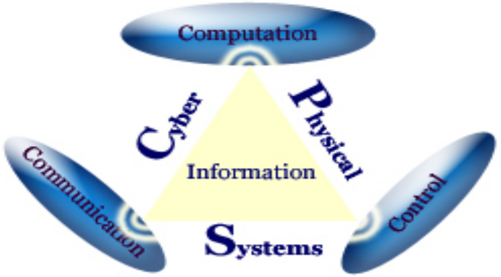
- Motivation
- Offline Modeling and Verification?
- Online Modeling and Verification
- Conclusion

Outline

- Motivation
- Offline Modeling and Verification?
- Online Modeling and Verification
- Conclusion

Motivation

- Cyber-Physical System

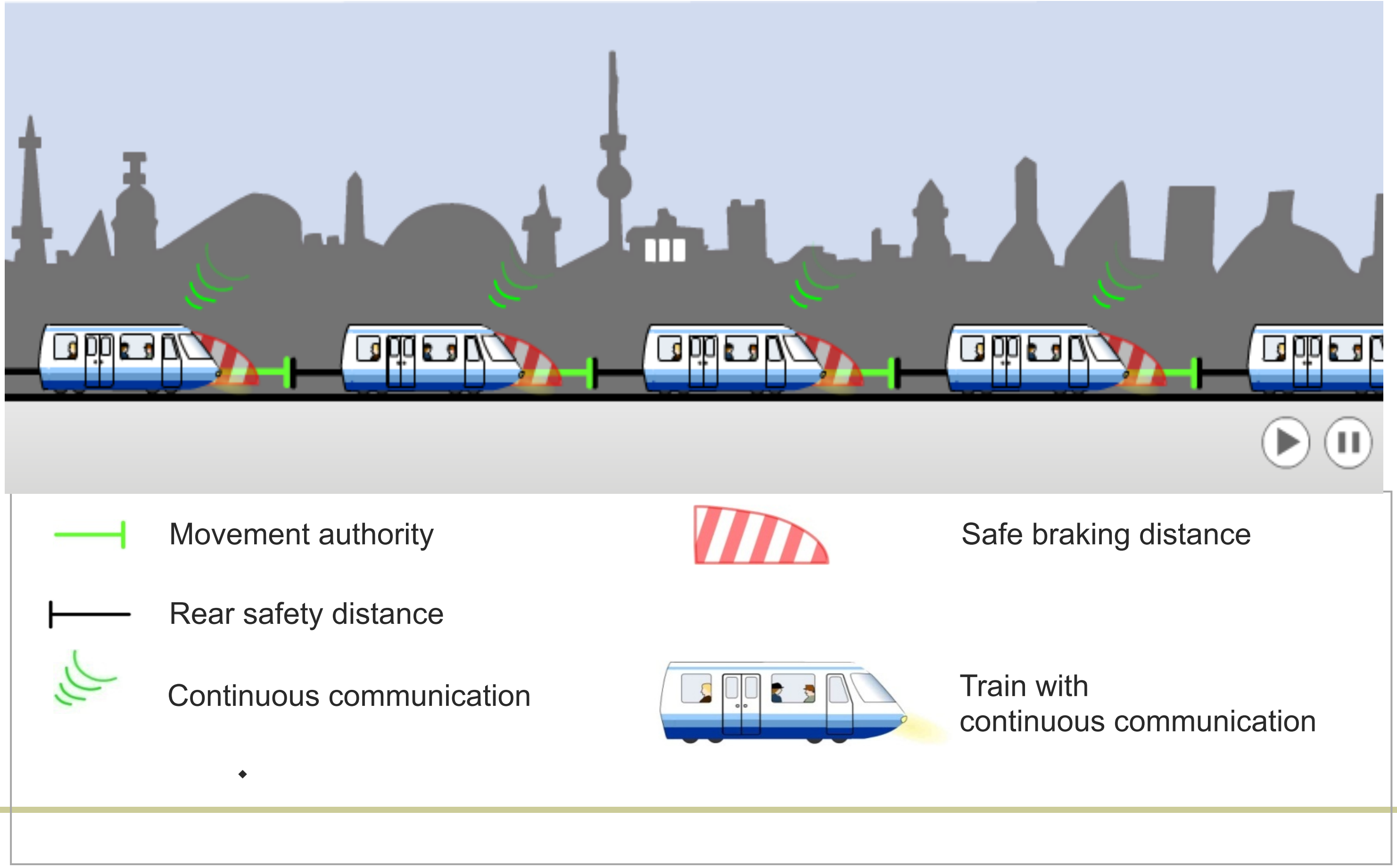


- Safety-Critical Area

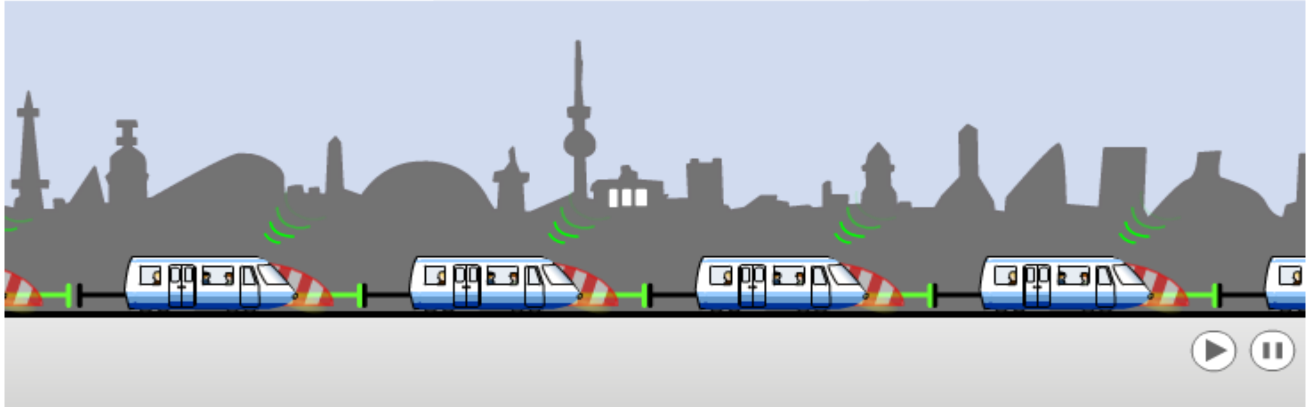
- Verification

Motivating Example 1

- Communication-Based Train Control System



- Train Control System

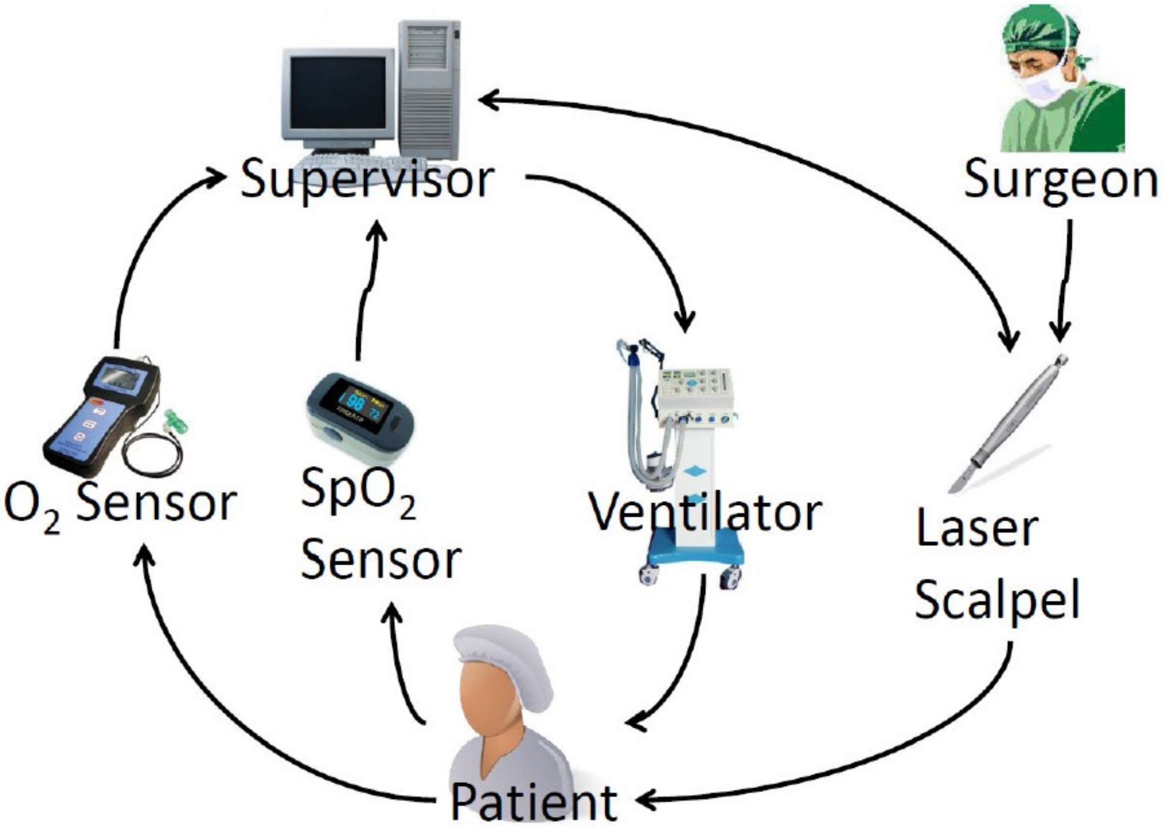


  - Train communicates with RBC for new MA by 500ms.
  - If a train touches a SBD point, brake normally.
  - If a train has not get any info for 5s, brake emergently!

- Specification
  - No Collision!

Motivating Example 2

- Medical Cyber Physical System

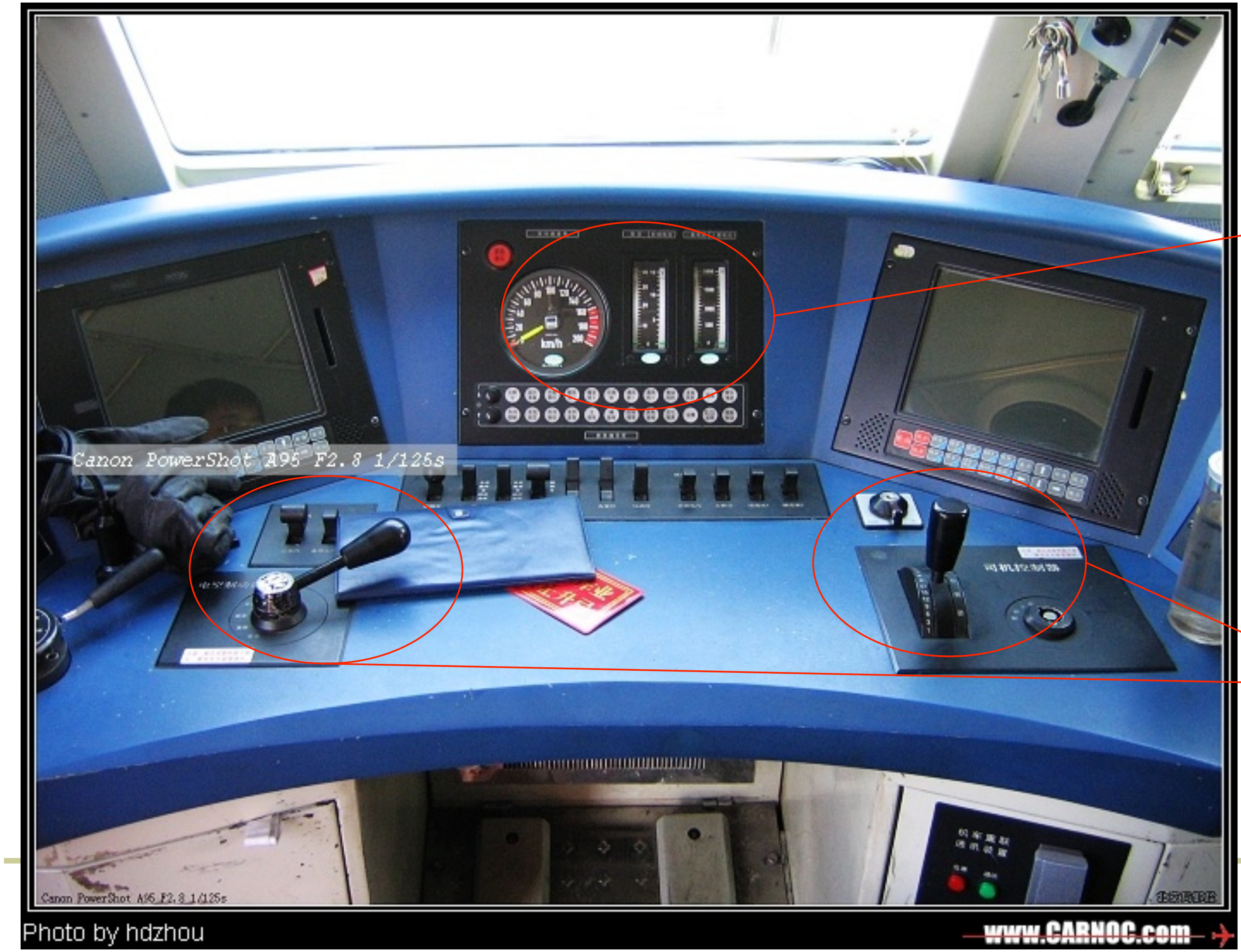


- Safety Rule
  - Safety Rule1: when the laser scalpel emits laser, the patient's trachea oxygen level must not exceed a threshold Θ_{O_2} Fire!
  - Safety Rule2: the patient's blood oxygen level never reaches below a threshold Θ_{SpO_2} Suffocation!

Outline

- Motivation
- Offline Modeling and Verification?
- Online Modeling and Verification
- Conclusion

Train



Continuous Realtime Behavior

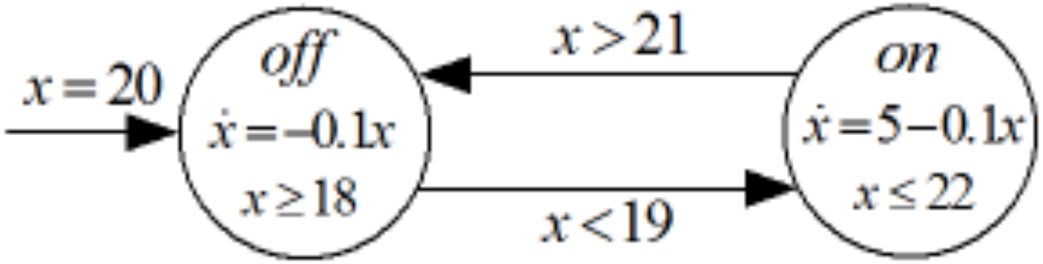
↓

Hybrid Behavior

↑

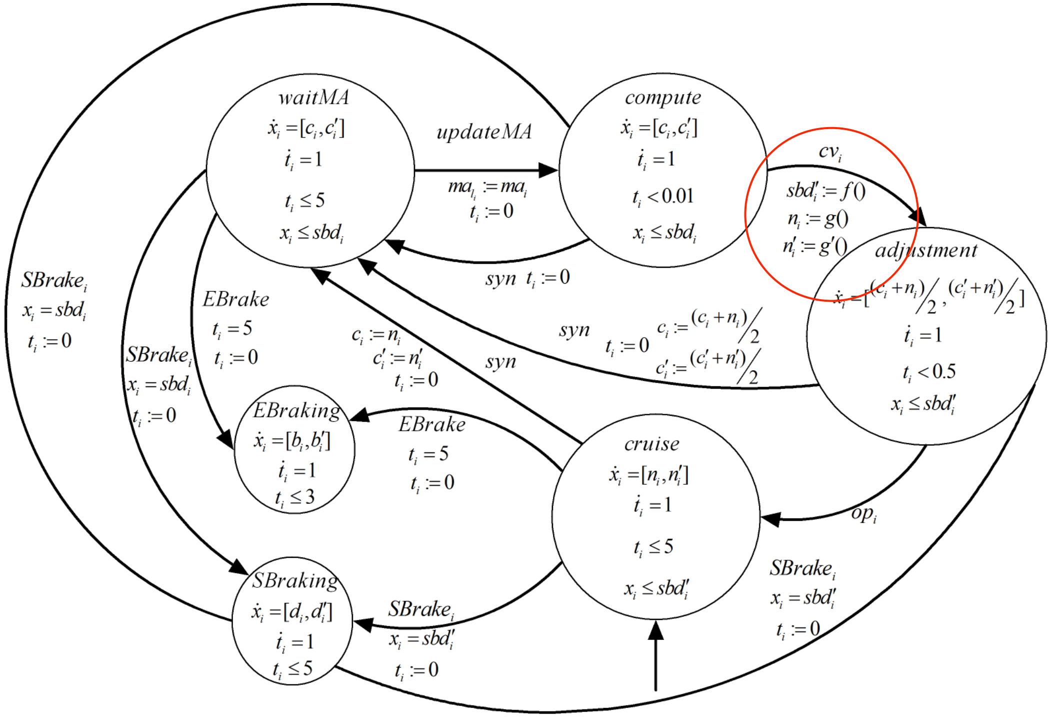
Discrete Logic Control

- Hybrid Automata
  - Discrete Logic Transition
  - Continuous Real-Timed Behavior
  - Most Natural Model for CPS System

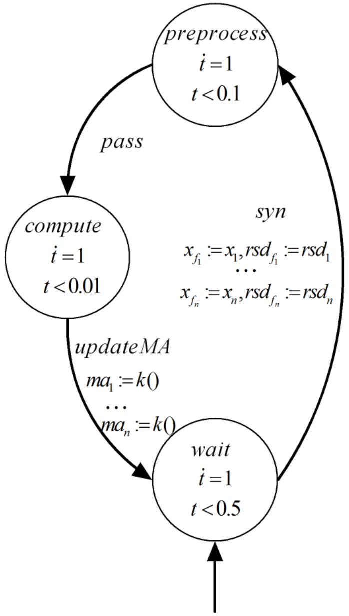


- Our Target
  - Model the Target CPS Systems by HA
  - Verify it by Model Checking

Modeling



(A)

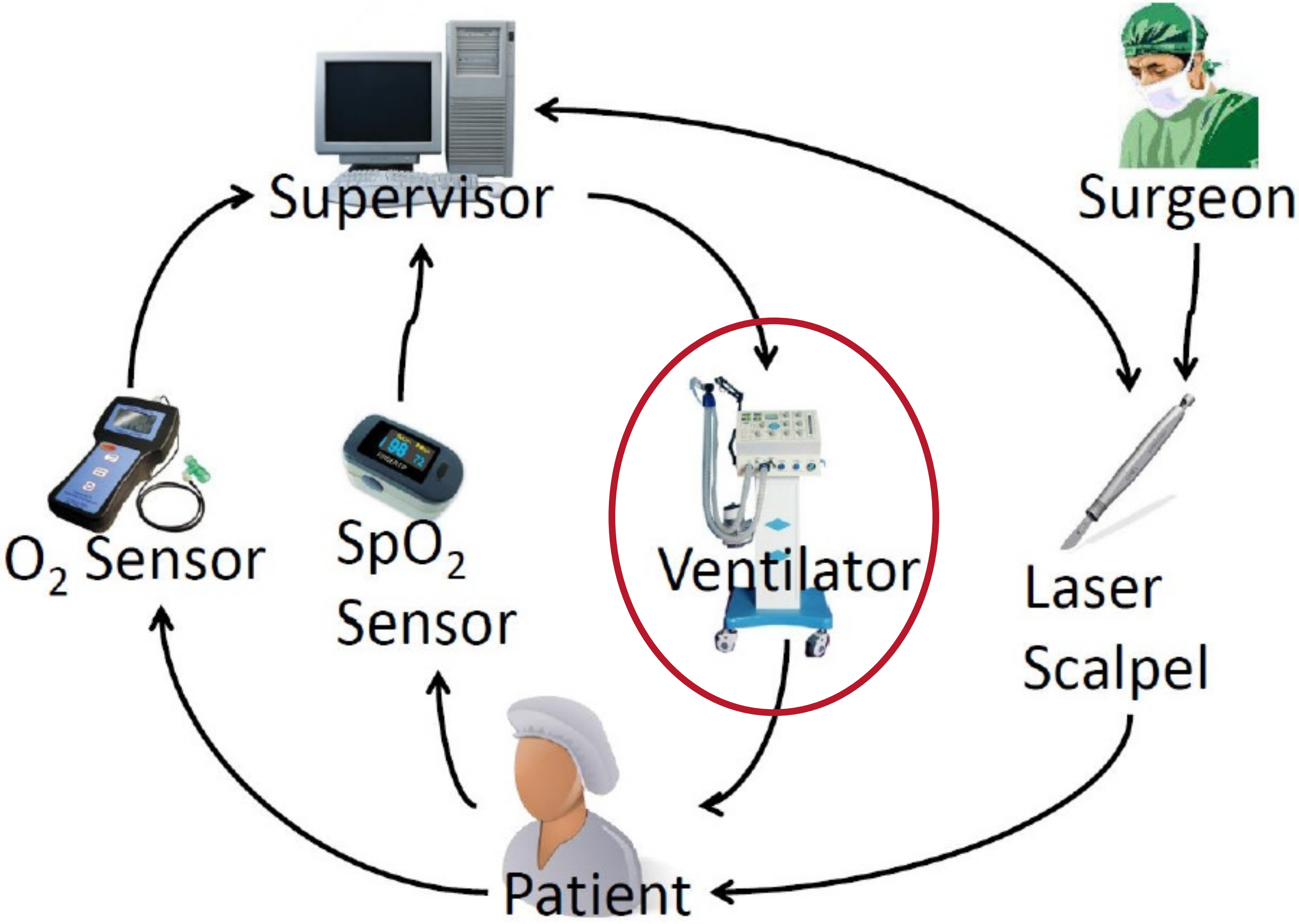


(B)

Specification：

Location: Sbraking; Constraint: Traini.x>ma

Problem: Lots of Free Parameters Included in the control functions: Windspeed , train mass, raining, etc..



Supervisor

Surgeon

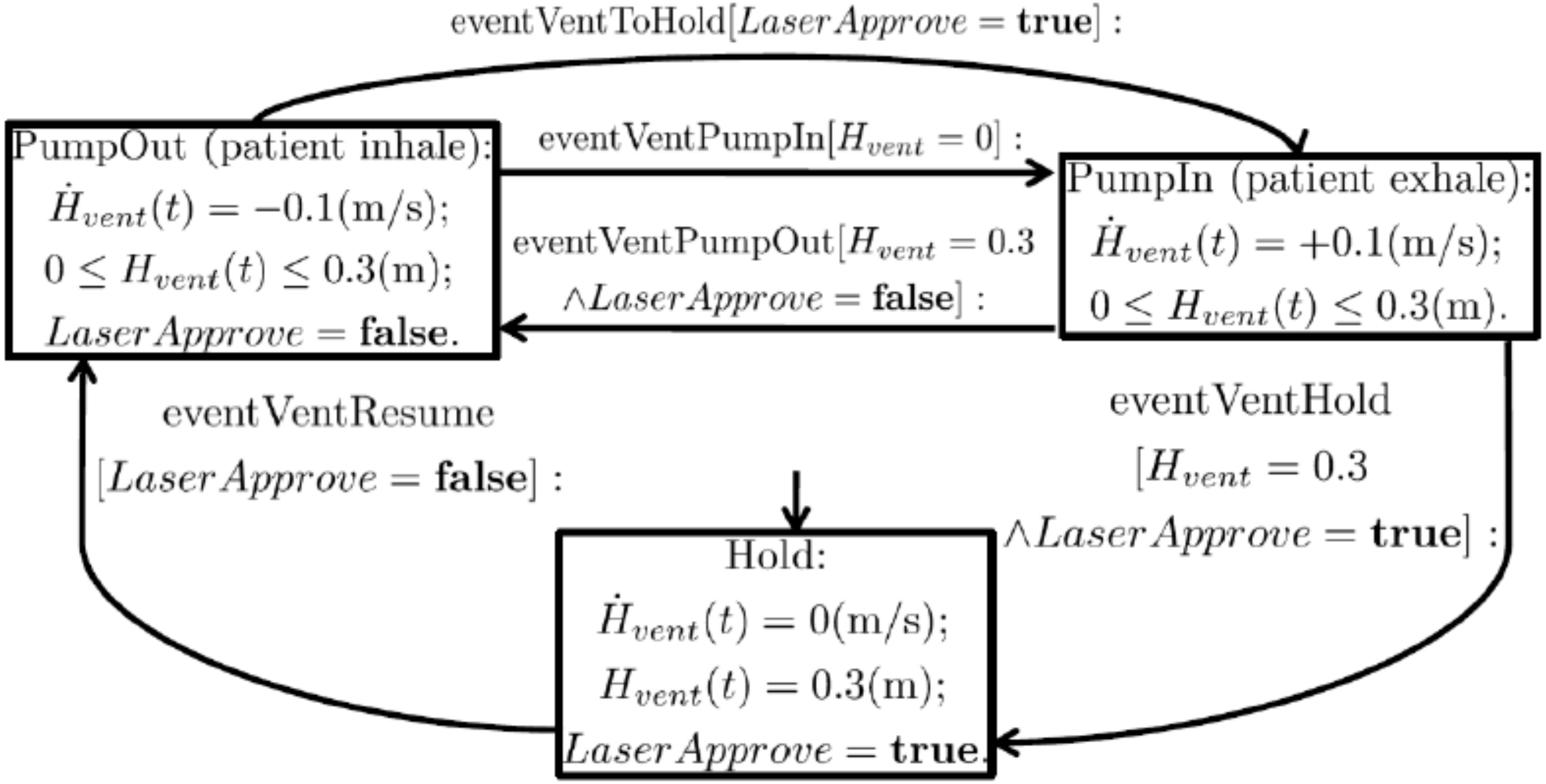
O_2 Sensor

SpO_2 Sensor

Ventilator

Laser Scalpel

Patient



eventVentToHold$[\mathit{LaserApprove} = \mathbf{true}]$:

PumpOut (patient inhale):
$\dot{H}_{vent}(t) = -0.1(\mathrm{m/s})$;
$0 \leq H_{vent}(t) \leq 0.3(\mathrm{m})$;
$\mathit{LaserApprove} = \mathbf{false}$.

eventVentPumpIn$[H_{vent} = 0]$:

eventVentPumpOut$[H_{vent} = 0.3$
$\wedge \mathit{LaserApprove} = \mathbf{false}]$:

PumpIn (patient exhale):
$\dot{H}_{vent}(t) = +0.1(\mathrm{m/s})$;
$0 \leq H_{vent}(t) \leq 0.3(\mathrm{m})$.

eventVentResume
$[\mathit{LaserApprove} = \mathbf{false}]$:

eventVentHold
$[H_{vent} = 0.3$
$\wedge \mathit{LaserApprove} = \mathbf{true}]$:

Hold:
$\dot{H}_{vent}(t) = 0(\mathrm{m/s})$;
$H_{vent}(t) = 0.3(\mathrm{m})$;
$\mathit{LaserApprove} = \mathbf{true}$.

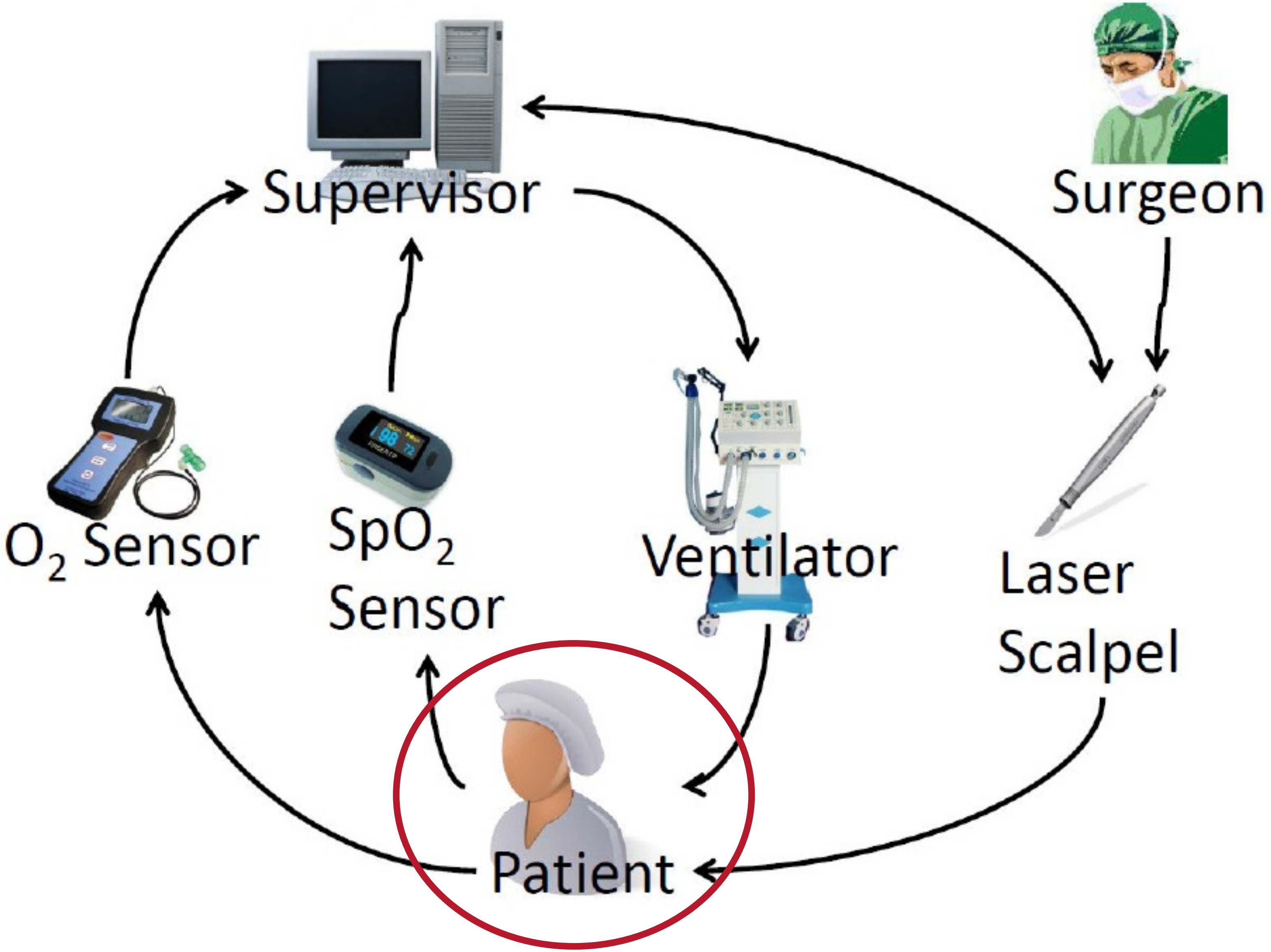
Legend:

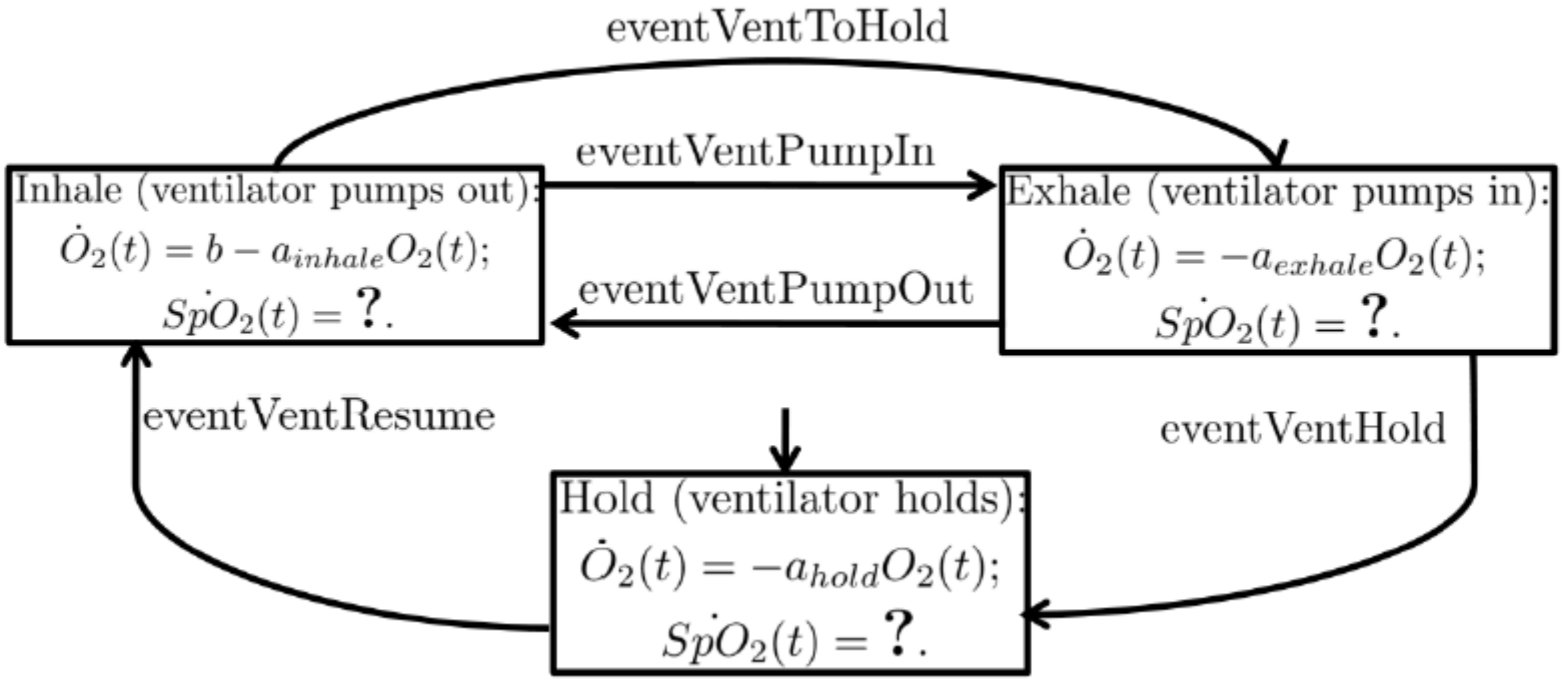
→ (w/ source location) Event; (w/o source location) Initial location indicator

□ Location

[ ] Event guard (event triggering condition)

:= Variable value update


Supervisor
Surgeon
O_2 Sensor
SpO_2 Sensor
Ventilator
Laser Scalpel
Patient


eventVentToHold
eventVentPumpIn
Inhale (ventilator pumps out):
$\dot{O}_2(t) = b - a_{inhale}O_2(t);$
$Sp\dot{O}_2(t) = ?.$
eventVentPumpOut
Exhale (ventilator pumps in):
$\dot{O}_2(t) = -a_{exhale}O_2(t);$
$Sp\dot{O}_2(t) = ?.$
eventVentResume
eventVentHold
Hold (ventilator holds):
$\dot{O}_2(t) = -a_{hold}O_2(t);$
$Sp\dot{O}_2(t) = ?.$

- Blood oxygen level is strongly affected by complex human body biochemical reactions, even emotions. No way to model SpO_2 in a long run

Outline

- Motivation
- Offline Modeling and Verification
- Online Modeling and Verification
- Conclusion

Solution

Online periodical real-time hybrid systems model checking of time-bounded (i.e., short-run) future!

Traditional model checking vs. Ours:

Offline	←→	Online Periodical Real-Time
Long-Run Future	←→	Short-Run Future

Challenge 1 : No good offline long run models for nondeterministic parameters .

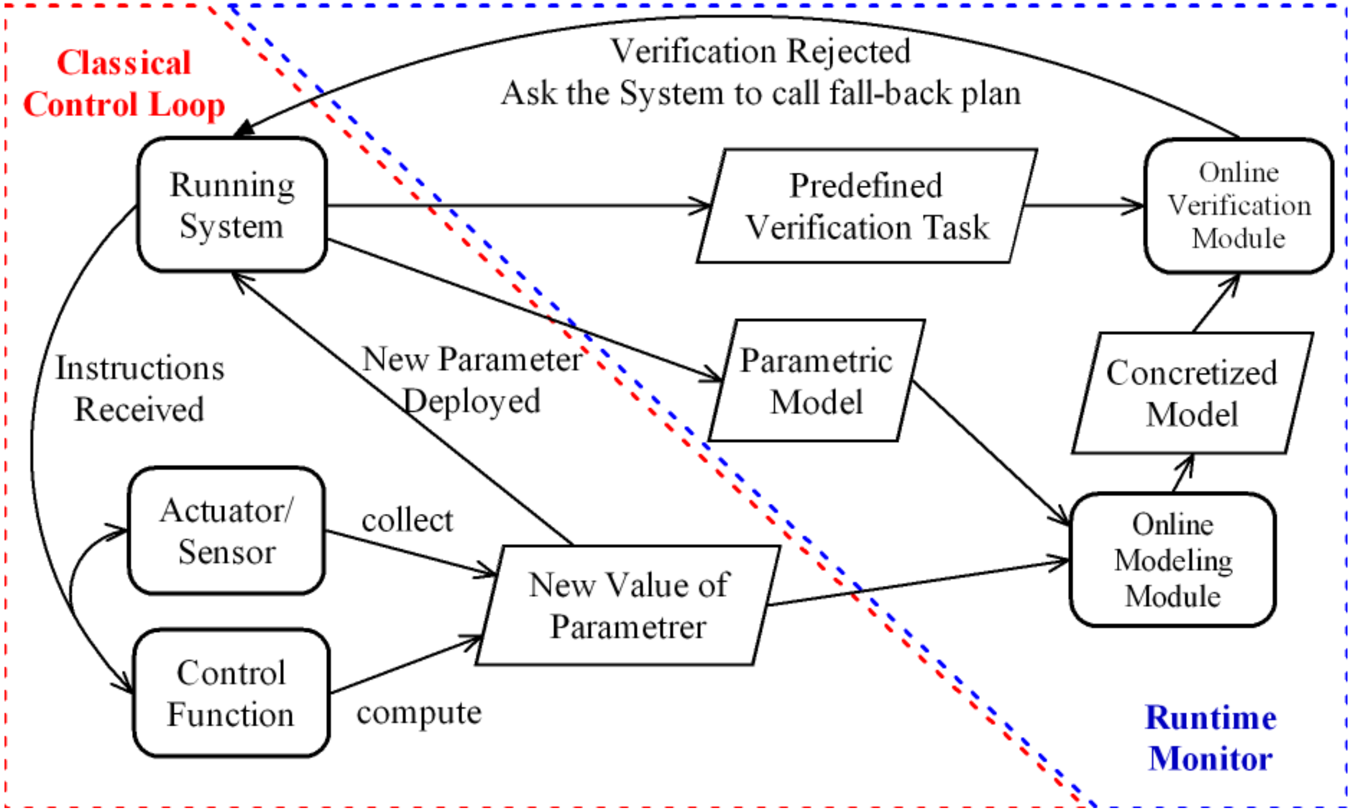
After the key parameters' values are fixed, the system's online short-run behavior is easy to predict.

Challenge 2: Verification state space easily explode.

Online → Fixes Many Parameters

Short-Run → Shrink State Space

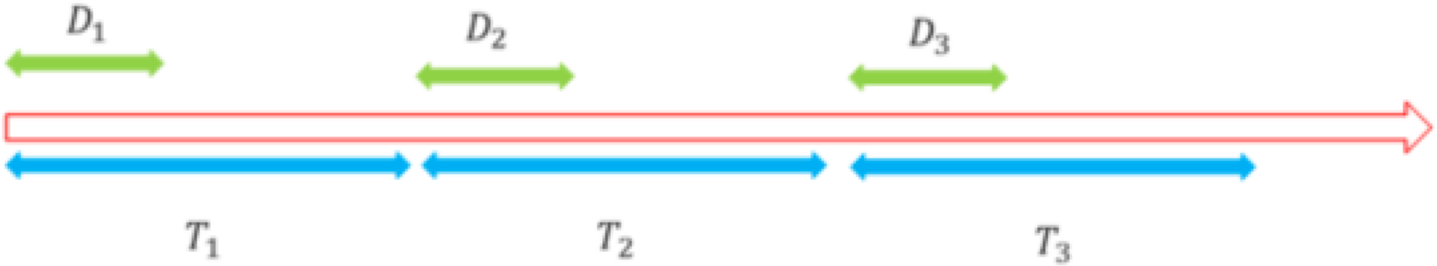
System Control



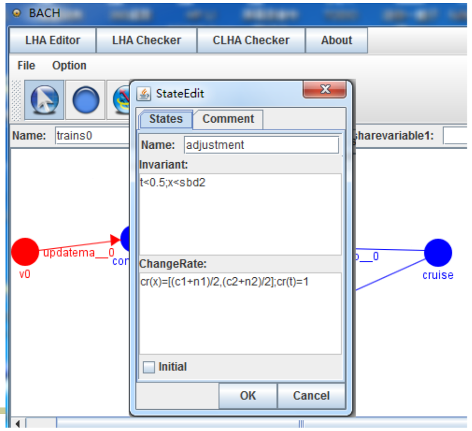
Performance Issue

- Periodically online verification -> Have to Be Fast!

- The model updates every T time unit, if we can not finish the online modeling and verification in D time unit, the result will be useless



- Multicore Assignment Distribution
- Incremental Online Verification
- Our Own Tool BACH$_{OL}$…



Name: trains0

Name: adjustment

Invariant:

t<0.5;x<sbd2

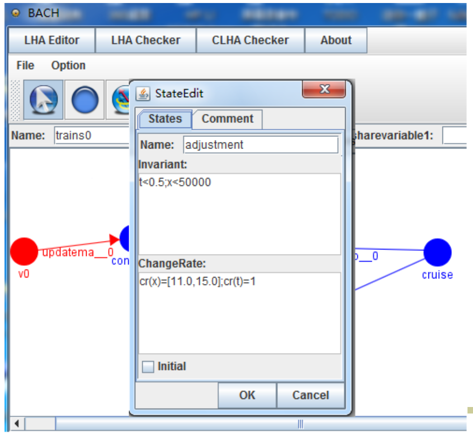
ChangeRate:

cr(x)=[(c1+n1)/2,(c2+n2)/2];cr(t)=1

□ Initial

sharevariable1:

(A)



Name: trains0

Name: adjustment

Invariant:

t<0.5;x<50000

ChangeRate:

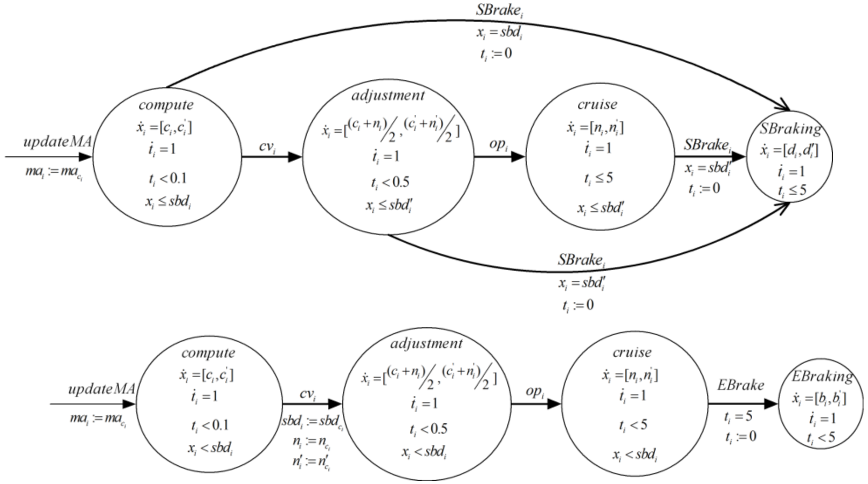
cr(x)=[11.0,15.0];cr(t)=1

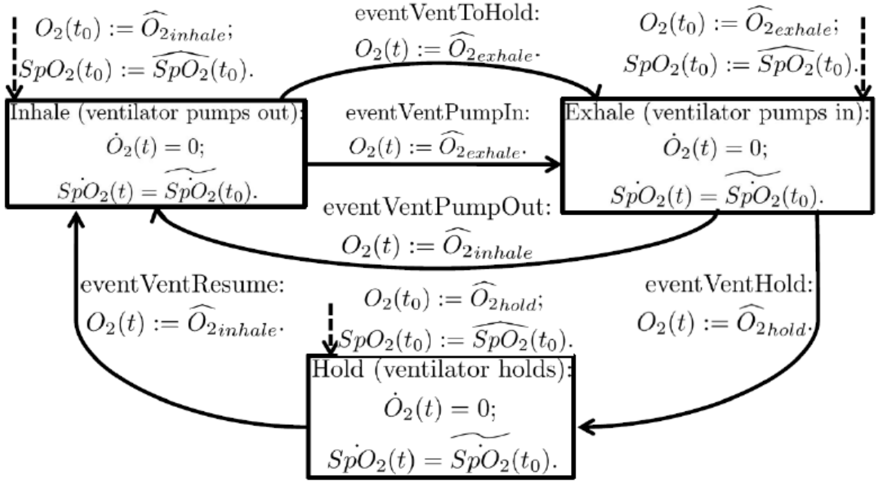
□ Initial

sharevariable1:

(B)

Evaluation


$SBrake_i$ $x_i = sbd_i$ $t_i := 0$
compute $\dot{x}_i = [c_i, c_i']$ $\dot{t}_i = 1$ $t_i < 0.1$ $x_i \le sbd_i$
updateMA $ma_i := ma_{c_i}$
cv_i
adjustment $\dot{x}_i = [(c_i + n_i)/2, (c_i' + n_i')/2]$ $\dot{t}_i = 1$ $t_i < 0.5$ $x_i \le sbd_i'$
op_i
cruise $\dot{x}_i = [n_i, n_i']$ $\dot{t}_i = 1$ $t_i \le 5$ $x_i \le sbd_i'$
$SBrake_i$ $x_i = sbd_i'$ $t_i := 0$
SBraking $\dot{x}_i = [d_i, d_i']$ $\dot{t}_i = 1$ $t_i \le 5$
$SBrake_i$ $x_i = sbd_i'$ $t_i := 0$
updateMA $ma_i := ma_{c_i}$
compute $\dot{x}_i = [c_i, c_i']$ $\dot{t}_i = 1$ $t_i < 0.1$ $x_i < sbd_i$
cv_i $sbd_i := sbd_{c_i}$ $n_i := n_{c_i}$ $n_i' := n_{c_i}'$
adjustment $\dot{x}_i = [(c_i + n_i)/2, (c_i' + n_i')/2]$ $\dot{t}_i = 1$ $t_i < 0.5$ $x_i < sbd_i$
op_i
cruise $\dot{x}_i = [n_i, n_i']$ $\dot{t}_i = 1$ $t_i < 5$ $x_i < sbd_i$
EBrake $t_i = 5$ $t_i := 0$
EBraking $\dot{x}_i = [b_i, b_i']$ $\dot{t}_i = 1$ $t_i < 5$


$O_2(t_0) := \widehat{O}_{2inhale}$; $SpO_2(t_0) := \widehat{SpO_2}(t_0)$.
eventVentToHold: $O_2(t) := \widehat{O}_{2exhale}$.
$O_2(t_0) := \widehat{O}_{2exhale}$; $SpO_2(t_0) := \widehat{SpO_2}(t_0)$.
Inhale (ventilator pumps out): $\dot{O}_2(t) = 0$; $\dot{SpO_2}(t) = \widetilde{\dot{SpO_2}}(t_0)$.
eventVentPumpIn: $O_2(t) := \widehat{O}_{2exhale}$.
Exhale (ventilator pumps in): $\dot{O}_2(t) = 0$; $\dot{SpO_2}(t) = \widetilde{\dot{SpO_2}}(t_0)$.
eventVentPumpOut: $O_2(t) := \widehat{O}_{2inhale}$
eventVentResume: $O_2(t) := \widehat{O}_{2inhale}$.
$O_2(t_0) := \widehat{O}_{2hold}$; $SpO_2(t_0) := \widehat{SpO_2}(t_0)$.
eventVentHold: $O_2(t) := \widehat{O}_{2hold}$.
Hold (ventilator holds): $\dot{O}_2(t) = 0$; $\dot{SpO_2}(t) = \widetilde{\dot{SpO_2}}(t_0)$.

Train Control System

10 train 109ms< 500ms

Laser Scalpel

932ms <4 s

（The first number is the mean value, the second number is the updating period ）

ICCPS 11 WIP, ICCPS 12, DSN 13, TPDS

- Motivation
- Offline Modeling and Verification
- Online Modeling and Verification
- Conclusion

Conclusion

- Offline M&V → Online M&V
- Non-deterministic -> Periodically deterministic
- Fast Verification
- Ongoing Work
  - Pipeline Design Based State Space Coverage

Thanks

Q&A