Dependable Hybrid Systems Design: a Refinement Approach

Zheng Cheng Dominique Méry

Nov, 2020

Where were we?

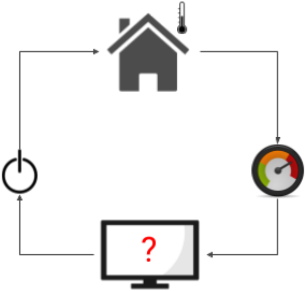
- Overview of hybrid system
- Review of calculus
- Review of Event-B
- Develop theories in Event-B

Outlines

Design Hybrid Systems in Event-B

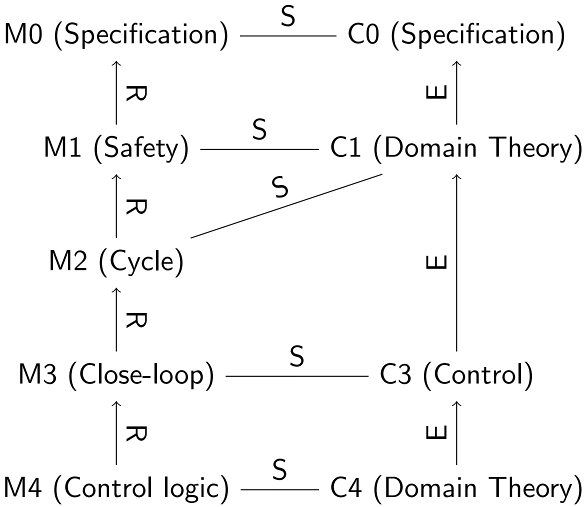
- Smart Heating System
- Refinement Strategy for Hybrid System Design

Smart Heating System



- 2 modes: ON/OFF
- Simple dynamics: $\dot{T}$=1/-1
- Sample at δ s
- Switch mode costs t_{act} s ($t_{act} < \delta$)
- Safety: $T_{min} \leq$ T $\leq T_{max}$

Refinement Strategy for Hybrid System Design

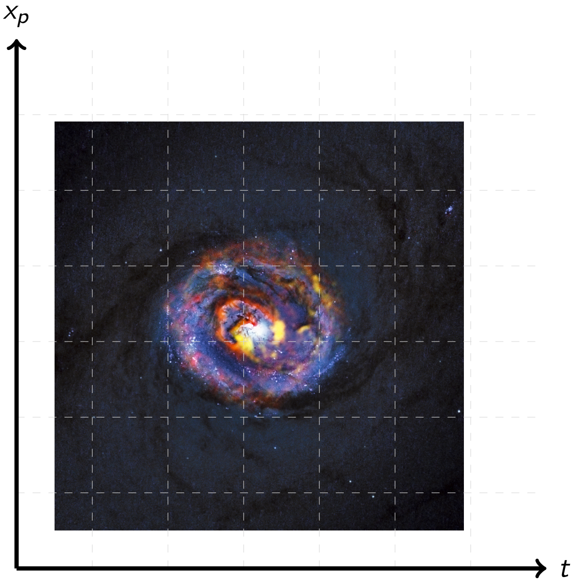


M0 (Specification)
S
C0 (Specification)
R
E
M1 (Safety)
S
C1 (Domain Theory)
S
R
M2 (Cycle)
E
R
M3 (Close-loop)
S
C3 (Control)
R
E
M4 (Control logic)
S
C4 (Domain Theory)

Lab Material

- `https://github.com/veriatl/LORIA_WEEK2`
- Import **theory-axiom-real** to Rodin, and deploy this theory
- Import **ex-heating-maintainer-event** to Rodin

Smart Heating System (Specification M0)

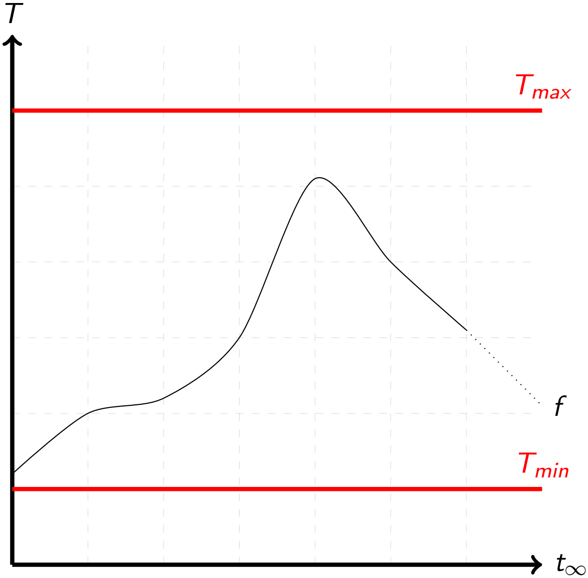


Smart Heating System (Specification M0)

Checklist:

- Generic hybrid system state trajectory
- Generic safety property
- Big-step semantics

Smart Heating System (Safety M1)

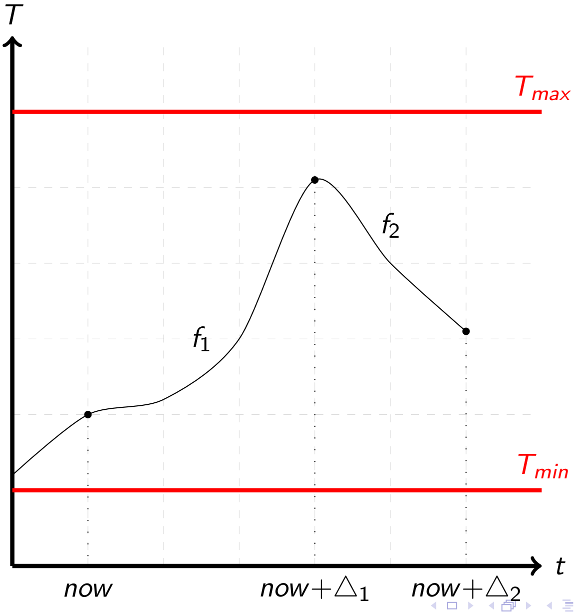


Smart Heating System (Safety M1)

Checklist:

- Concrete system state trajectory
- Concrete safety property
- Big-step semantics refined
- Important proof obligations: guard preservation

Smart Heating System (Cycle M2)

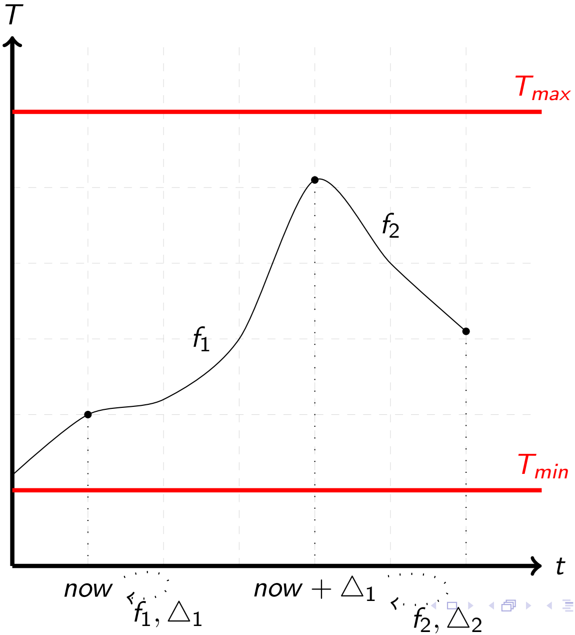


Smart Heating System (Cycle M2)

Checklist:

- Time pointer
- Refined system state trajectory
- Refined safety property
- Small-step semantics
- Important proof obligations: invariant preservation

Smart Heating System (Close-loop M3)



Smart Heating System (Close-loop M3)

Checklist:

- Variable for close-loop mode control
- Prediction (Controller)
- Progression (Plant)

Smart Heating System (Control Logic M4)

Event-triggered

Checklist:

- Event-triggered design(when certain events are detected what actions that system should take)
- Specification of time-triggered design

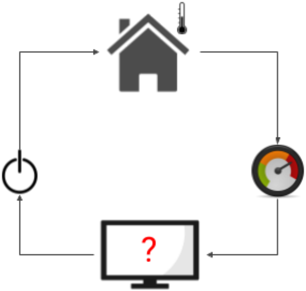
Smart Heating System (Control Logic M4)

Time-triggered

Checklist:

- Revisit the description of heating system
- Time-triggered design(the controller takes action only every once in a while)

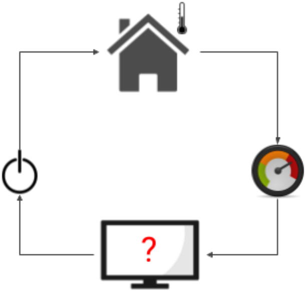
Smart Heating System (Revisit)



- 2 modes: ON/OFF

→ the only actuation we can do

Smart Heating System (Revisit)



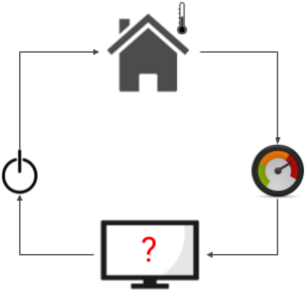
- 2 modes: ON/OFF

→ the only actuation we can do

- Simple dynamics: $\dot{T}$=1/-1

→ monotonicity

Smart Heating System (Revisit)



- 2 modes: ON/OFF

→ the only actuation we can do

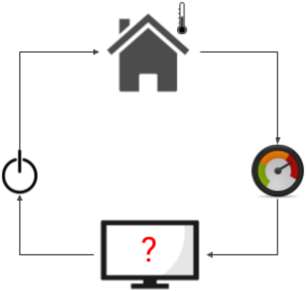
- Simple dynamics: $\dot{T}$=1/-1

→ monotonicity

- Sample at δ s

→ Decision at sampling time

Smart Heating System (Revisit)



- 2 modes: ON/OFF

→ the only actuation we can do

- Simple dynamics: $\dot{T}$=1/-1

→ monotonicity

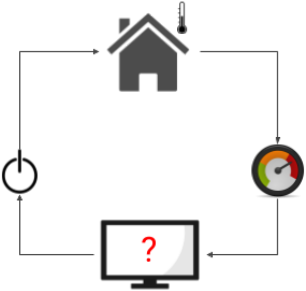
- Sample at δ s

→ Decision at sampling time

- Switch mode costs t_{act} s ($t_{act} < \delta$)

→ Cost of switch mode

Smart Heating System (Revisit)



- 2 modes: ON/OFF

→ the only actuation we can do

- Simple dynamics: $\dot{T}$=1/-1

→ monotonicity

- Sample at δ s

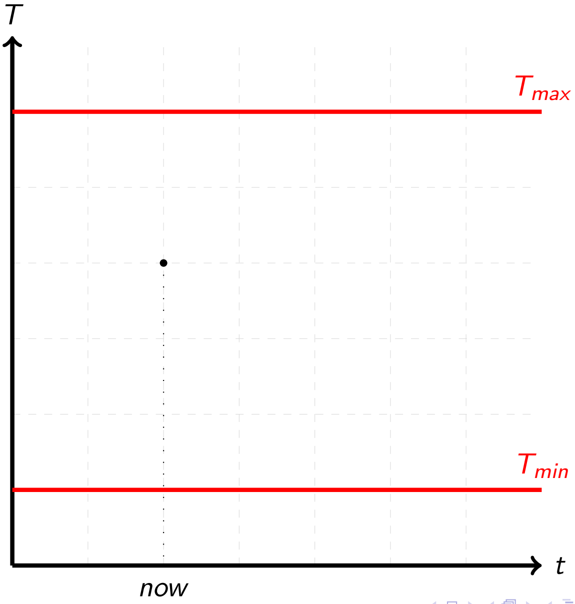
→ Decision at sampling time

- Switch mode costs t_{act} s ($t_{act} < \delta$)

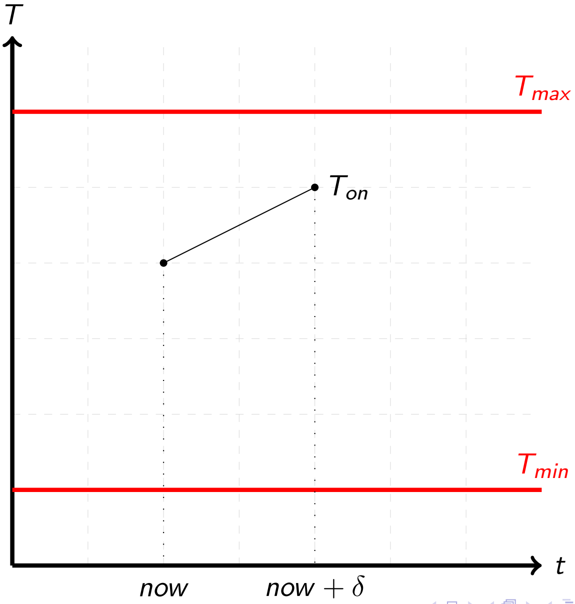
→ Cost of switch mode

- Safety: $T_{min} \leq$ T $\leq$ T_{max}

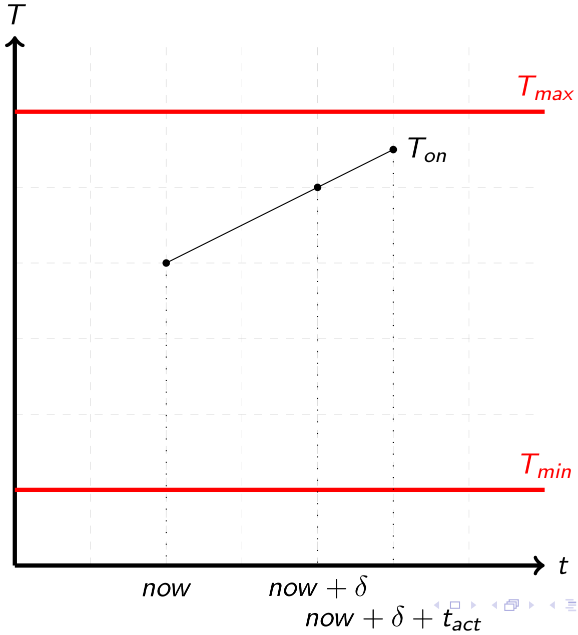
Case 1: ON mode, $T(now) \leq T_{max}$, Stay ON



Case 1: ON mode, $T(now + \delta) \leq T_{max}$, Stay ON



Case 1: ON mode, $T(now + \delta + t_{act}) \leq T_{max}$, Stay ON



Case 2,3,4: ?