Dependable Hybrid Systems Design: a Refinement Approach

Dominique Méry   Zheng Cheng

Jan 27th, 2020

Where were we?

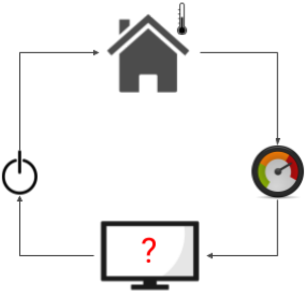
- Overview of hybrid system
- Review of calculus
- Review of Event-B
- Develop theories in Event-B

Outlines

Design Hybrid Systems in Event-B

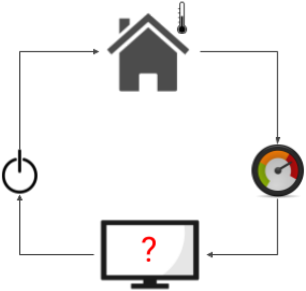
- Smart Heating System
- Refinement Strategy for Hybrid System Design

Smart Heating System



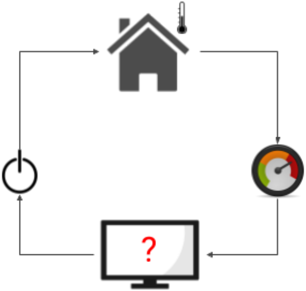
- 2 modes: ON/OFF

Smart Heating System



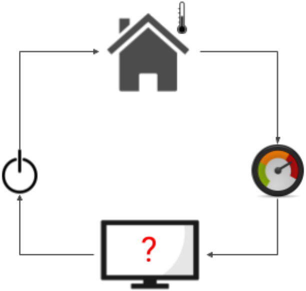
- 2 modes: ON/OFF
- Simple dynamics: $\dot{T}$=1/-1

Smart Heating System



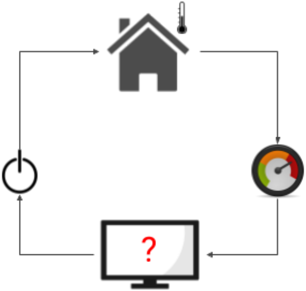
- 2 modes: ON/OFF
- Simple dynamics: $\dot{T}$=1/-1
- Sample at δ s

Smart Heating System



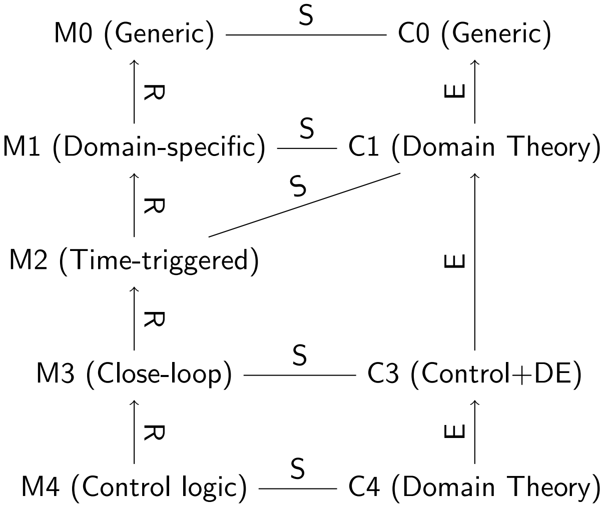
- 2 modes: ON/OFF
- Simple dynamics: $\dot{T}$=1/-1
- Sample at δ s
- Switch mode costs t_{act} s ($t_{act} < \delta$)

Smart Heating System

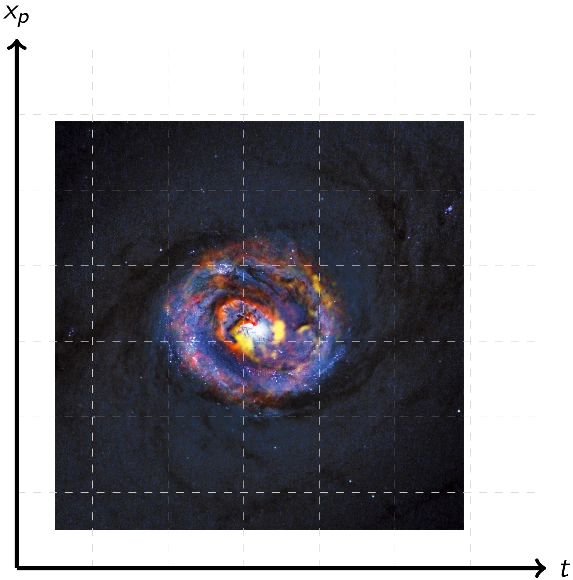


- 2 modes: ON/OFF
- Simple dynamics: $\dot{T}$=1/-1
- Sample at δ s
- Switch mode costs t_{act} s ($t_{act} < \delta$)
- Safety: $T_{min} \leq$ T $\leq T_{max}$

Refinement Strategy for Hybrid System Design



Smart Heating System (Generic M0)

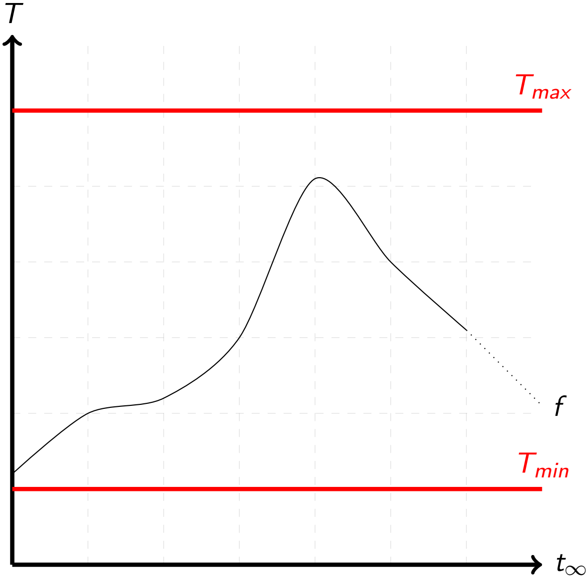


Smart Heating System (Generic M0)

Checklist:

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

Smart Heating System (Domain-specific M1)

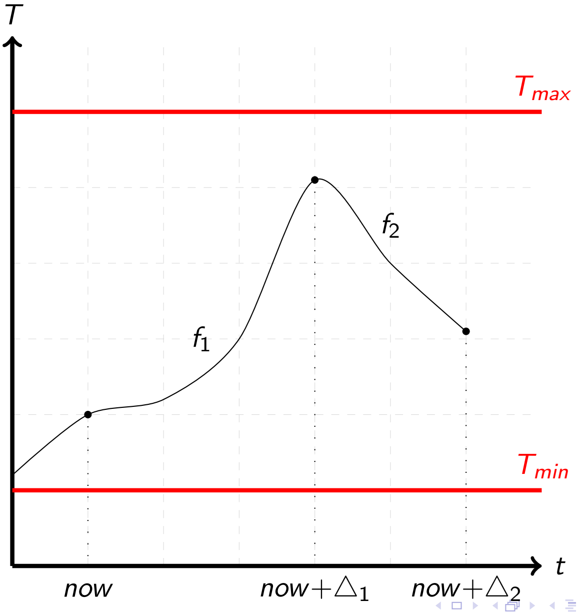


Smart Heating System (Domain-specific M1)

Checklist:

- Concrete system state trajectory
- Concrete safety property
- Big-step semantics
- Data refinement
- Proof obligations

Smart Heating System (Time-triggered M2)

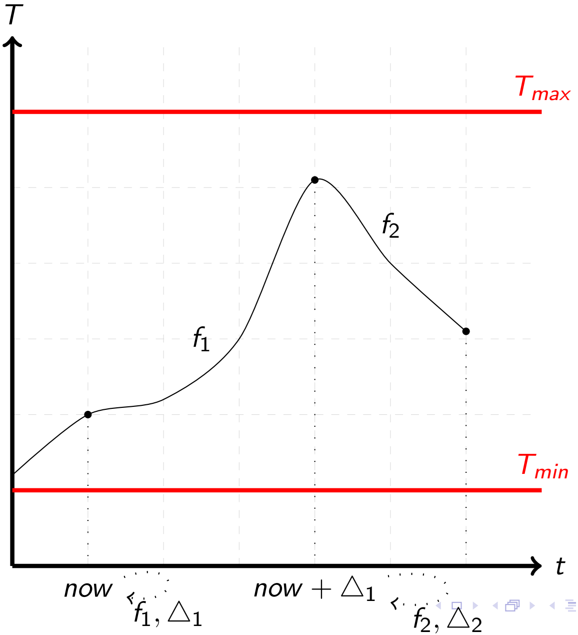


Smart Heating System (Time-triggered M2)

Checklist:

- Time pointer
- Refined system state trajectory
- Refined safety property
- Small-step semantics
- Invariant preservation
- Lab Practice: `https://github.com/veriatl/LORIA_WEEK2`

Smart Heating System (Close-loop M3)



Smart Heating System (Close-loop M3)

Checklist:

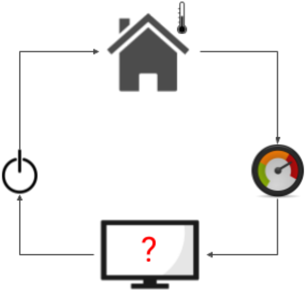
- Variable for close-loop mode control
- Prediction (Controller)
- Progression (Plant)

Smart Heating System (Control Logic M4)

Checklist:

- Revisit the description of heating system
- Complete case analysis

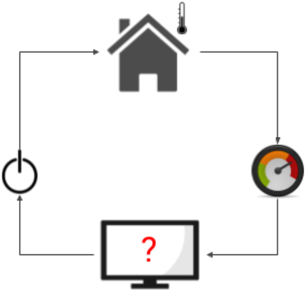
Smart Heating System (Revisit)



- 2 modes: ON/OFF

→ the only actuation we can do

Smart Heating System (Revisit)



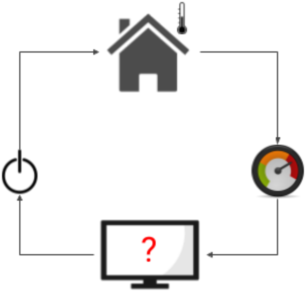
- 2 modes: ON/OFF

→ the only actuation we can do

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

→ monotonicity

Smart Heating System (Revisit)



- 2 modes: ON/OFF

$\rightarrow$ the only actuation we can do

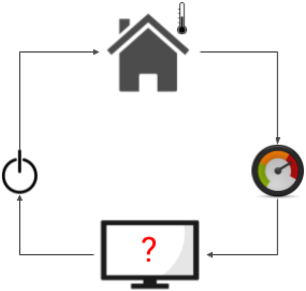
- Simple dynamics: $\dot{T}$=1/-1

$\rightarrow$ monotonicity

- Sample at δ s

$\rightarrow$ 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

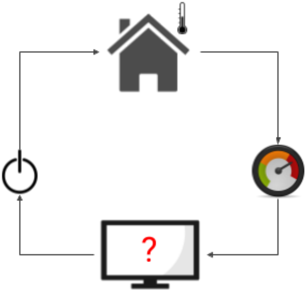
- Sample at δ s

→ 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

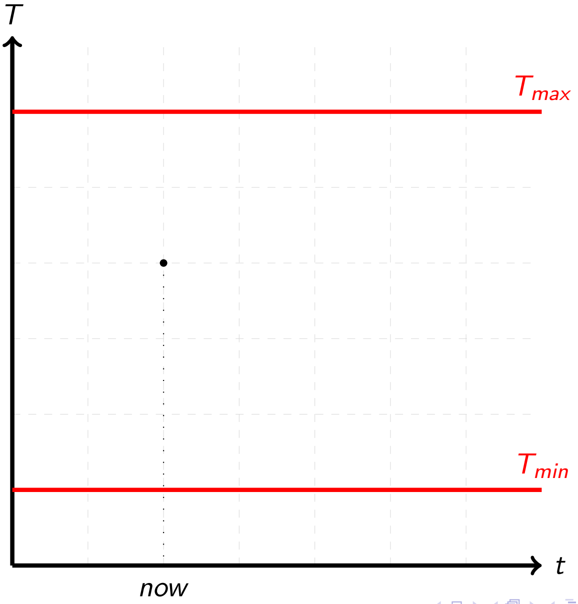
→ Decision at sampling time

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

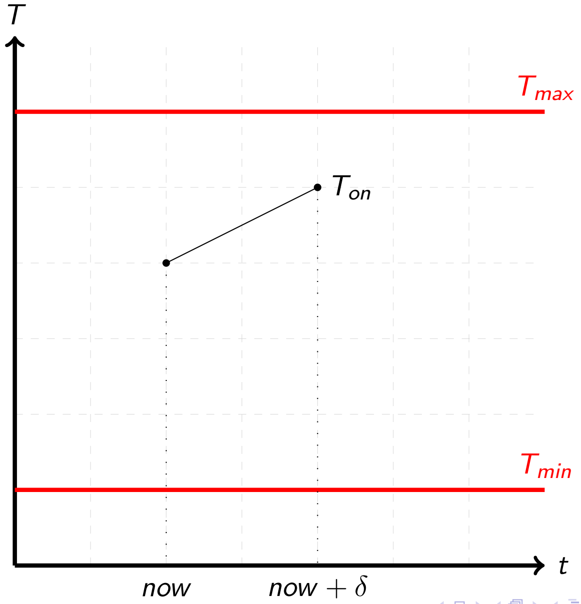
→ Cost of switch mode

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

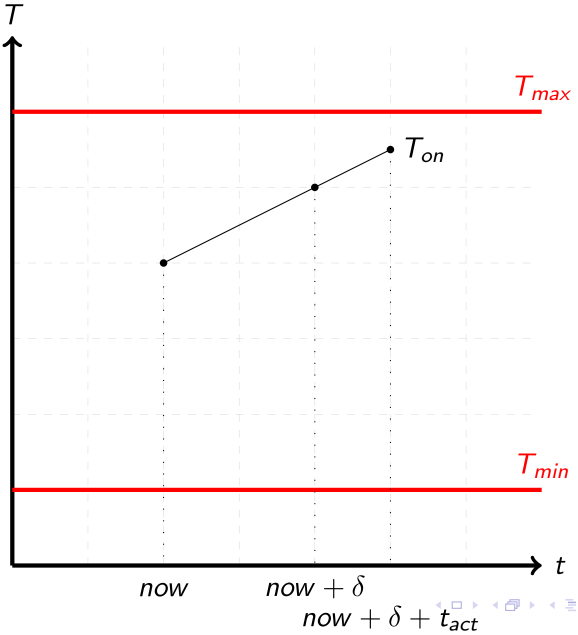
Case 1: ON mode, $T(now) \leq T_{max}$, Stay ON



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



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



Case 2: ?