Computer Science Master Thesis Proposals UCSP

Marco Muñiz

Aalborg University

June 26, 2018

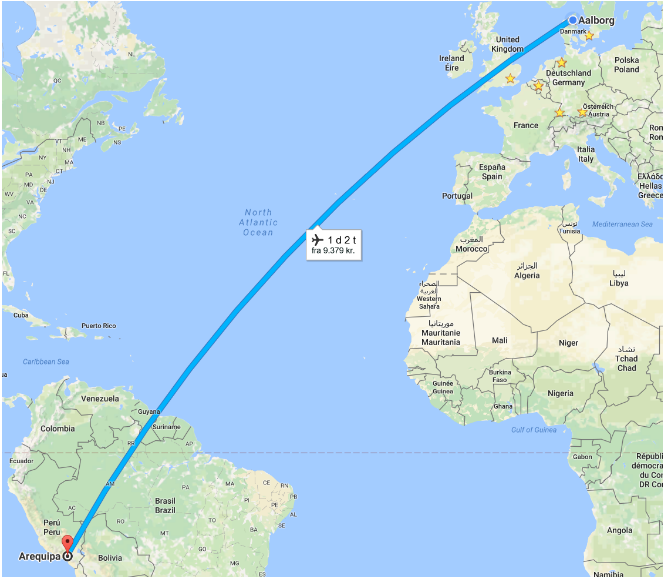
About Marco Muñiz [1]

Research interests span the areas of modeling, formal verification, and synthesis.

- *Post doctoral researcher*
  Aalborg University, 2015-now
- *Dr. ret nat. in Computer Science*
  University of Freiburg, Germany, 2009-2015
  Thesis: Model Checking for Time Division Multiple Access Systems
  Advisor: Prof. Dr. Andreas Podelski
- *M.Sc. in Computer Science*
  University of Freiburg, Germany, 2006-2009
  Thesis: Decision Procedures for List Manipulating Programs
  Advisor: Prof. Dr. Andreas Podelski and Prof. Dr. Thomas Wies
- *Systems Engineer*
  Saint Mary Catholic University, Arequipa, Peru, 1998-2004

[1] `http://people.cs.aau.dk/~muniz/`

Aalborg, Denmark



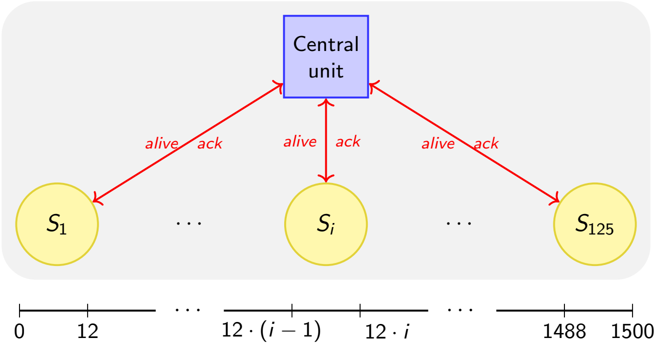
Aalborg, Denmark

Distributed Embeded Intelligent Systems [2]

[2] http://www.cs.aau.dk/research/distributed-embedded-intelligent-systems/

Case Study: Fire Alarm System from SeCa GmbH

Wireless TDMA based communication protocol

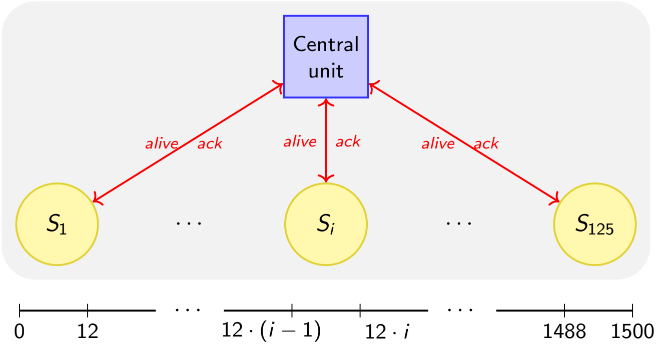


Safety Critical Systems

Unexpected behavior can cost human lives or catastrophic economical losses. Correct functioning is a prime concern.

Case Study: Fire Alarm System from SeCa GmbH

Fire alarm system in surveillance mode

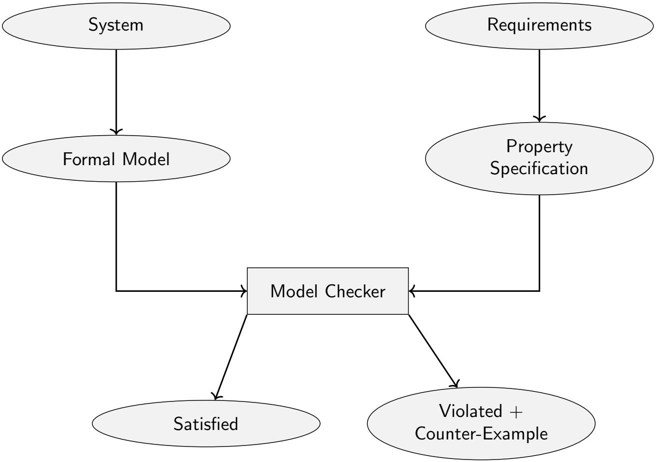


Real Time Requirement (EN 54)

If a sensor malfunctions, the malfunction should be detected by the central unit in less than 3000 time units from the begin of failure.

Model Checking

Successful technique for automatically verifying correctness properties of finite-state systems.



Modeling the System with Timed-Arc Petri Nets

Timed-Arc Petri Nets is a formalism to model and verify real-time systems.

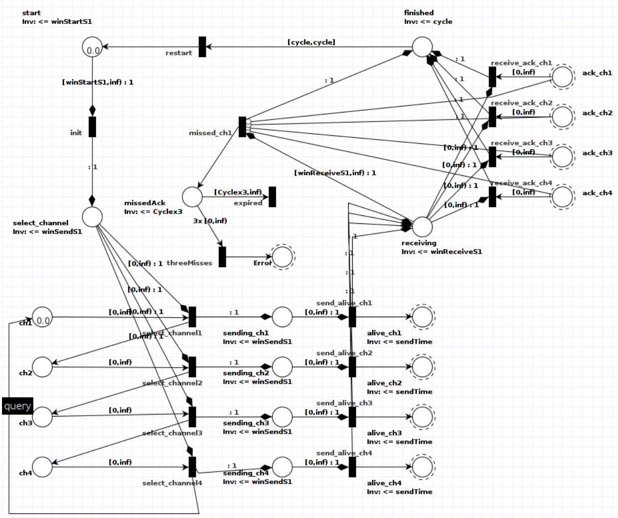
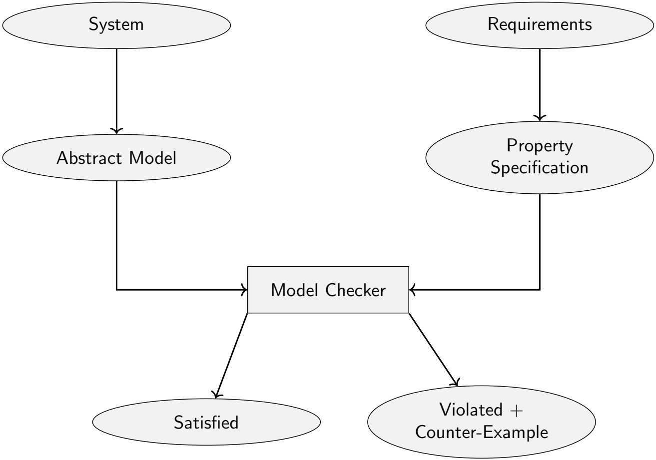


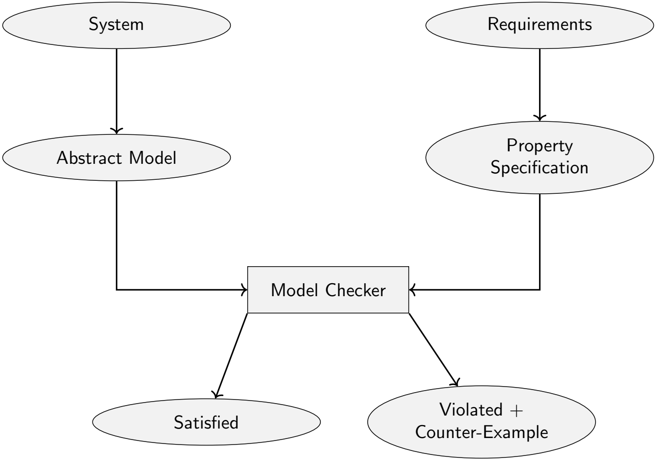
Figure: A Timed-Arc Petri Net for sensor1 from the fire alarm system.

Model Checking the Fire Alarm System

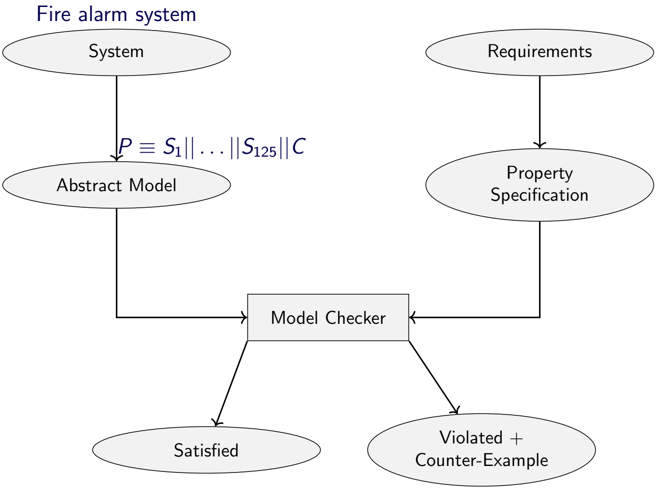


Model Checking the Fire Alarm System

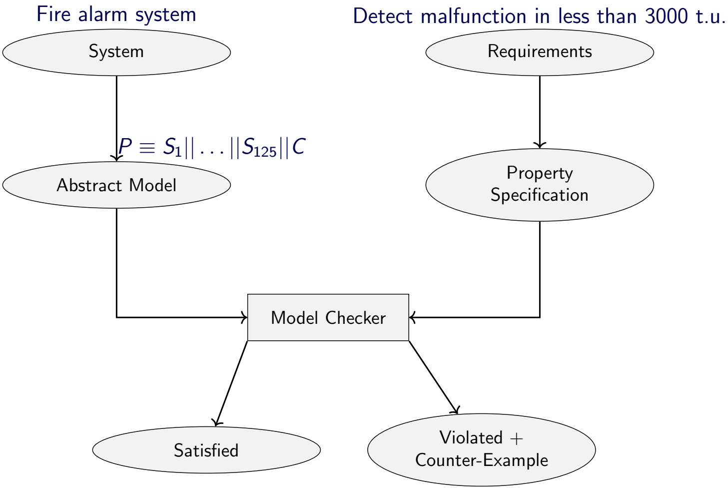
Fire alarm system



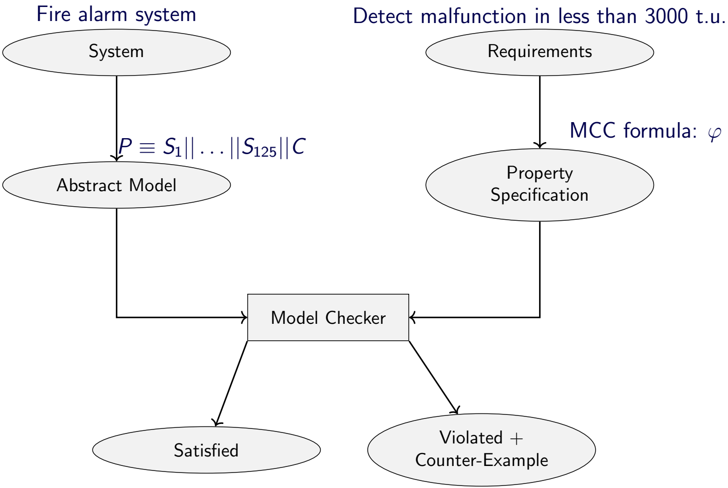
Model Checking the Fire Alarm System



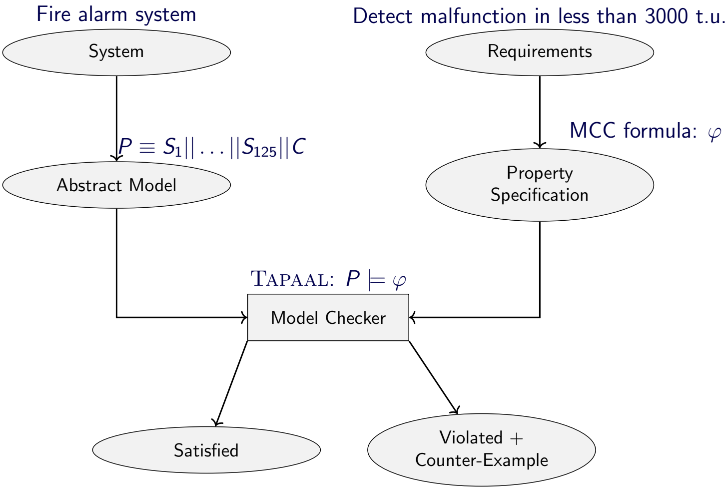
Model Checking the Fire Alarm System



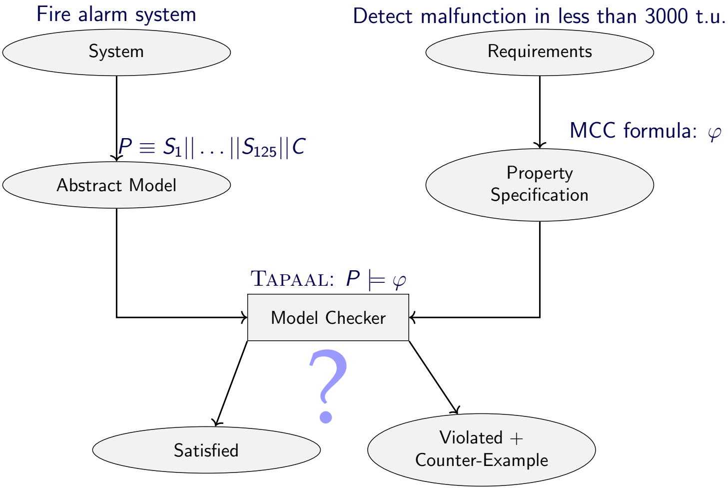
Model Checking the Fire Alarm System



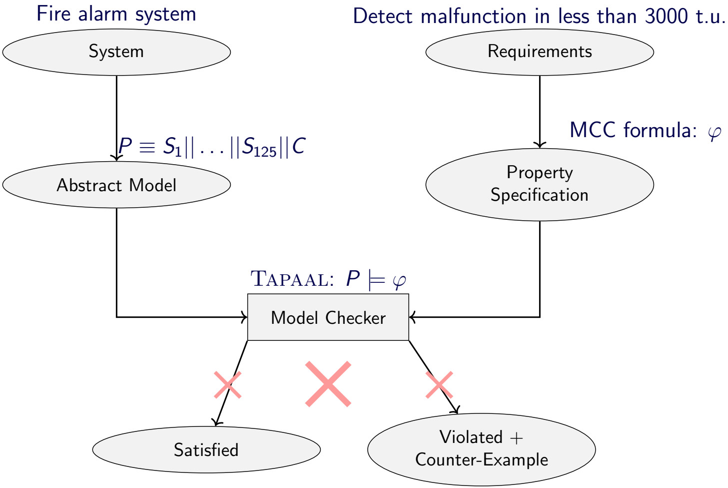
Model Checking the Fire Alarm System



Model Checking the Fire Alarm System

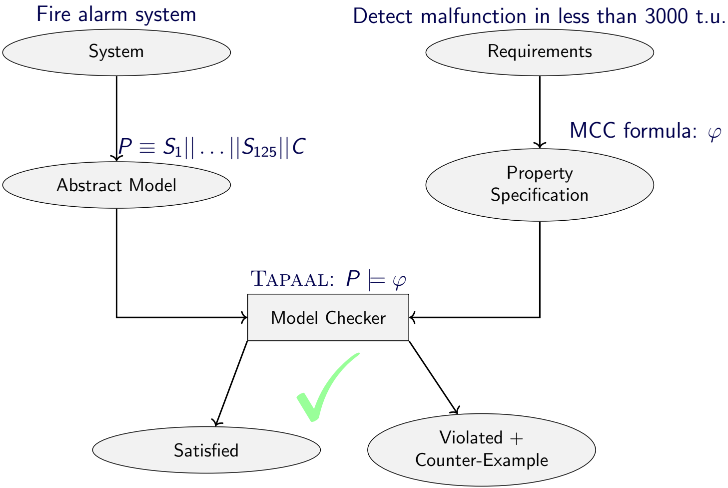


Model Checking the Fire Alarm System



Problem: size of the model hinders the verification task

Model Checking the Fire Alarm System



Partial Order Reduction (POR)

Partial Order Reduction [God91, Lip75, Maz87, Pel93, Val91] is a successful technique in combating the state space explosion problem

Independence of Actions (intuition)

Actions are independent iff

- they do not disable or enable each other,
- they commute.

Partial Order Reduction (POR)

Partial Order Reduction [God91, Lip75, Maz87, Pel93, Val91] is a successful technique in combating the state space explosion problem

Independence of Actions (intuition)

Actions are independent iff

- they do not disable or enable each other,
- they commute.

Consider two actions $a_1, a_2 \in A$ and a state $s \in S$.

$$s \xrightarrow{a_1} \circ$$

Partial Order Reduction (POR)

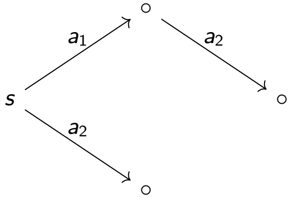
Partial Order Reduction [God91, Lip75, Maz87, Pel93, Val91] is a successful technique in combating the state space explosion problem

Independence of Actions (intuition)

Actions are independent iff

- they do not disable or enable each other,
- they commute.

Consider two actions $a_1, a_2 \in A$ and a state $s \in S$.



Partial Order Reduction (POR)

Partial Order Reduction [God91, Lip75, Maz87, Pel93, Val91] is a successful technique in combating the state space explosion problem

Independence of Actions (intuition)

Actions are independent iff

- they do not disable or enable each other,
- they commute.

Consider two actions $a_1, a_2 \in A$ and a state $s \in S$.

$$\begin{tikzcd} & \circ \arrow[dr, "a_2"] & \\ s \arrow[ur, "a_1"] \arrow[dr, "a_2"'] & & \circ \\ & \circ \arrow[ur, "a_1"'] & \end{tikzcd}$$

Partial Order Reduction

Reduction (intuition)

A reduction is a function $\mathsf{St} : S \rightarrow 2^A$ from states to sets of actions.

$\mathcal{R}$	Reduction preserves goal states
$\mathcal{W}$	Actions not in St are independent from actions in St

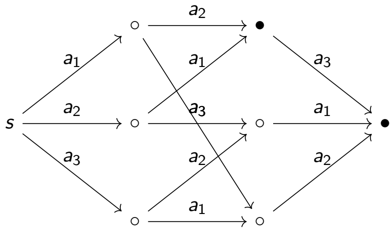
Partial Order Reduction

Reduction (intuition)

A reduction is a function $\mathrm{St} : S \to 2^A$ from states to sets of actions.

$\mathcal{R}$	Reduction preserves goal states
$\mathcal{W}$	Actions not in St are independent from actions in St

Assume $a_1, a_2, a_3 \in A$ are independent and $\bullet$ states are goal states.



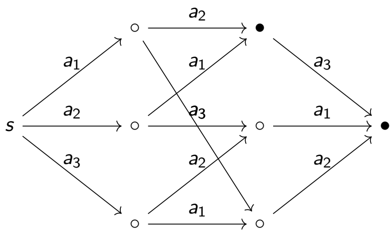
Partial Order Reduction

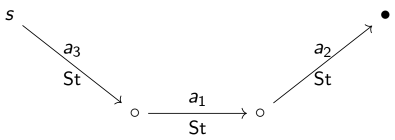
Reduction (intuition)

A reduction is a function $\mathsf{St} : S \to 2^A$ from states to sets of actions.

$\mathcal{R}$	Reduction preserves goal states
$\mathcal{W}$	Actions not in St are independent from actions in St

Assume $a_1, a_2, a_3 \in A$ are independent and $\bullet$ states are goal states.





Non reachability preserving reduction

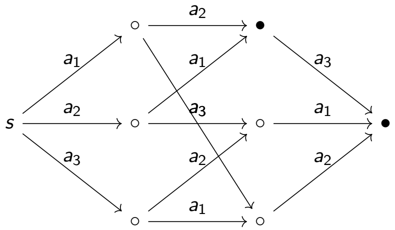
Partial Order Reduction

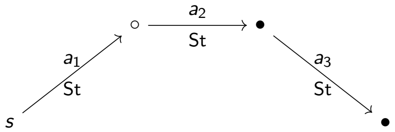
Reduction (intuition)

A reduction is a function $\mathrm{St} : S \to 2^A$ from states to sets of actions.

$\mathcal{R}$	Reduction preserves goal states
$\mathcal{W}$	Actions not in St are independent from actions in St

Assume $a_1, a_2, a_3 \in A$ are independent and $\bullet$ states are goal states.





Reachability preserving reduction

Partial Order Reduction for Timed Systems

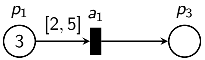
Success of POR has been challenged by the dependencies introduced by time elapsing

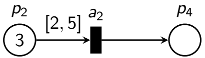
- In [BJLY98, Min99] local time semantics are assumed.
- In [SBM06, HLL^{+}14] over-approximations are computed.

Partial Order Reduction for Timed Systems

Success of POR has been challenged by the dependencies introduced by time elapsing

- In [BJLY98, Min99] local time semantics are assumed.
- In [SBM06, HLL$^+$14] over-approximations are computed.

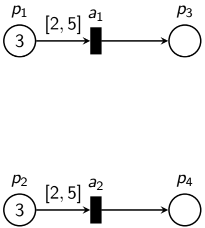


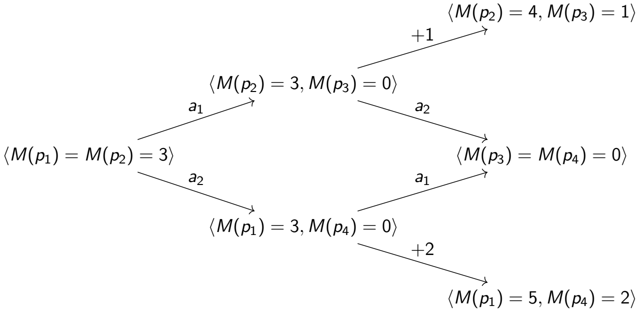


Partial Order Reduction for Timed Systems

Success of POR has been challenged by the dependencies introduced by time elapsing

- In [BJLY98, Min99] local time semantics are assumed.
- In [SBM06, HLL$^+$14] over-approximations are computed.





Partial Order Reduction for Timed Systems

Zero Time Partial Order Reduction CAV18 [BJL+18]

Reduction (intuition)

A reduction is a function $\mathrm{St} : S \to 2^A$ from states to sets of actions.

$\mathcal{Z}$	**If time can elapse, no reduction**
$\mathcal{D}$	**Reduction preserves states which can delay**
$\mathcal{R}$	Reduction preserves goal states
$\mathcal{W}$	Actions not in St are independent from actions in St

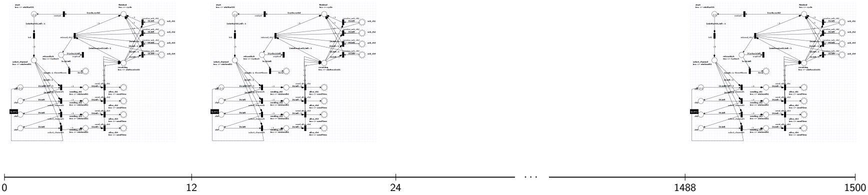
Partial Order Reduction for Timed Systems

Zero Time Partial Order Reduction CAV18 [BJL+18]

Reduction (intuition)

A reduction is a function $\mathrm{St} : S \to 2^A$ from states to sets of actions.

$\mathcal{Z}$	**If time can elapse, no reduction**
$\mathcal{D}$	**Reduction preserves states which can delay**
$\mathcal{R}$	Reduction preserves goal states
$\mathcal{W}$	Actions not in St are independent from actions in St



$$\langle M(p_{1,1}) = \cdots = M(p_{125,1}) = 0 \rangle \to^* \underbrace{\langle M(p_{1,end}) = \cdots = M(p_{125,end}) = 1500 \rangle}_{\text{zero time}}$$

Partial Order Reduction for Timed Systems

Results for Timed Arc Petri Nets in TAPAAL

	Time (seconds)		Markings ×1000		Reduction	
Model	NORMAL	POR	NORMAL	POR	%Time	%Markings
PatientMonitoring 3	5.88	0.35	333	28	94	92
PatientMonitoring 4	22.06	0.48	1001	36	98	96
PatientMonitoring 5	80.76	0.65	3031	44	99	99
PatientMonitoring 6	305.72	0.85	9248	54	100	99
PatientMonitoring 7	5516.93	5.75	130172	318	100	100
BloodTransfusion 2	0.32	0.41	48	43	-28	11
BloodTransfusion 3	7.88	6.45	792	546	18	31
BloodTransfusion 4	225.18	109.30	14904	7564	51	49
BloodTransfusion 5	5256.01	1611.14	248312	94395	69	62
FireAlarm 10	28.95	14.17	796	498	51	37
FireAlarm 12	116.97	17.51	1726	526	85	70
FireAlarm 14	598.89	21.65	5367	554	96	90
FireAlarm 16	5029.25	29.48	19845	582	99	97
FireAlarm 18	27981.90	34.55	77675	610	100	99
FireAlarm 20	154495.29	41.47	308914	638	100	100
FireAlarm 80	$>$ 2 days	602.71	-	1522	-	-
FireAlarm 125	$>$ 2 days	1957.00	-	2260	-	-

Partial Order Reduction for Timed Systems

Results for Timed Arc Petri Nets in TAPAAL

	Time (seconds)		Markings ×1000		Reduction	
Model	NORMAL	POR	NORMAL	POR	%Time	%Markings
BAwPC 2	0.21	0.41	19	16	-95	15
BAwPC 4	3.45	4.04	193	125	-17	35
BAwPC 6	23.01	17.08	900	452	26	50
BAwPC 8	73.73	39.29	2294	952	47	58
BAwPC 10	135.62	60.66	3819	1412	55	63
BAwPC 12	173.09	73.53	4736	1665	58	65
Fischer-9	3.24	2.37	281	233	27	17
Fischer-11	12.68	8.73	923	738	31	20
Fischer-13	42.52	28.53	2628	2041	33	22
Fischer-15	121.31	77.50	6700	5066	36	24
Fischer-17	313.69	198.36	15622	11536	37	26
Fischer-19	748.52	456.30	33843	24469	39	28
Fischer-21	1622.69	985.07	68934	48904	39	29
LynchShavit 9	3.98	3.31	282	234	17	17
LynchShavit 11	15.73	12.19	925	740	23	20
LynchShavit 13	51.08	37.97	2631	2043	26	22
LynchShavit 15	146.63	103.63	6703	5069	29	24
LynchShavit 17	384.52	258.09	15626	11540	33	26
LynchShavit 19	907.60	597.68	33848	24474	34	28
LynchShavit 21	2011.58	1307.72	68940	48910	35	29

Partial Order Reduction for Timed Systems

Results for Timed Arc Petri Nets in TAPAAL

	Time (seconds)		Markings $\times 1000$		Reduction	
Model	NORMAL	POR	NORMAL	POR	%Time	%Markings
MPEG2 3	13.17	15.43	2188	2187	-17	0
MPEG2 4	109.62	125.45	15190	15180	-14	0
MPEG2 5	755.54	840.84	87568	87478	-11	0
MPEG2 6	4463.19	5092.58	435023	434354	-14	0
AlternatingBit 20	9.17	9.51	617	617	-4	0
AlternatingBit 30	48.20	49.13	2804	2804	-2	0
AlternatingBit 40	161.18	162.94	8382	8382	-1	0
AlternatingBit 50	408.34	408.86	19781	19781	0	0

Thesis Proposal

Zero Time Partial Order Reduction CAV18 [BJL+18]

Reduction (intuition)

A reduction is a function $\mathrm{St} : S \to 2^A$ from states to sets of actions.

$\mathcal{Z}$	**If time can elapse, no reduction**
$\mathcal{D}$	**Reduction preserves states which can delay**
$\mathcal{R}$	Reduction preserves goal states
$\mathcal{W}$	Actions not in St are independent from actions in St (persistent sets)

Thesis Proposal

Zero Time Partial Order Reduction CAV18 [BJL+18]

Reduction (intuition)

A reduction is a function $\mathsf{St} : S \to 2^A$ from states to sets of actions.

$\mathcal{Z}$	**If time can elapse, no reduction**
$\mathcal{D}$	**Reduction preserves states which can delay**
$\mathcal{R}$	Reduction preserves goal states
$\mathcal{W}$	Actions not in St are independent from actions in St (persistent sets)

Comparing source sets vs. persistent sets [AAJS17]

Thesis Proposal

Zero Time Partial Order Reduction CAV18 [BJL^{+}18]

Reduction (intuition)

A reduction is a function $\mathrm{St} : S \to 2^A$ from states to sets of actions.

- $\mathcal{Z}$ **If time can elapse, no reduction**
- $\mathcal{D}$ **Reduction preserves states which can delay**
- $\mathcal{R}$ Reduction preserves goal states
- $\mathcal{W}$ Actions not in St are independent from actions in St (persistent sets)

Comparing source sets vs. persistent sets [AAJS17]

Objectives: Use source sets instead of persistent sets, provide an efficient algorithm for computing source sets TAPN, perform experiments.

Partial Order Reduction with Source Sets for Timed-arc Petri Nets

A reduction is a function $\mathrm{St} : S \to 2^A$ from states to sets of actions.

- $\mathcal{Z}$ **If time can elapse, no reduction**
- $\mathcal{D}$ **Reduction preserves states which can delay**
- $\mathcal{R}$ Reduction preserves goal states
- $\mathcal{S}$ source sets

1. About

2. Partial Order Reduction with Source Sets for Timed-Arc Petri Nets
   - Case Study: Fire Alarm System
   - Partial Order Reduction for Timed-Arc Petri Nets
   - Thesis Proposal: POR with Source Sets for Timed-arc Petri Nets

3. Synthesis of Optimal Controllers for Hybrid Solar Water Heating Systems
   - Case Study: Floor Heating System
   - Strategy Synthesis
   - Thesis Proposal: Synthesis of Optimal Controllers for Hybrid Solar Water Heating Systems

Case Study: Floor Heating System from Seluxit Aps

Case Study: Floor Heating System from Seluxit Aps

Relevant factors to consider

- Outside temperature, doors opening and closing
- Pipes heating a room may influence other rooms
- Pressure constraints

Case Study: Floor Heating System from Seluxit Aps

Current Operation

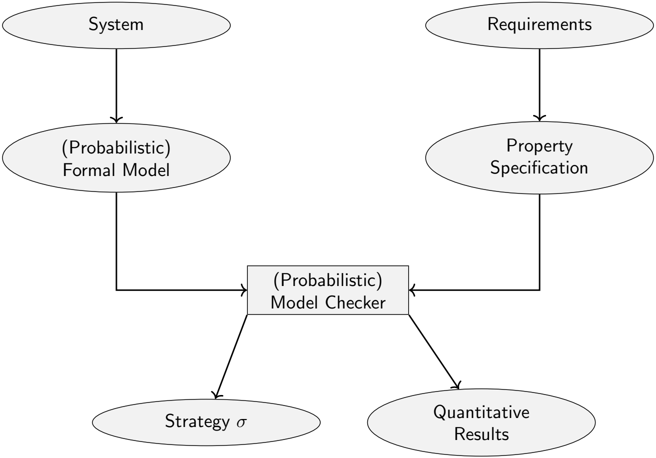
- Every 15 minutes there is a reading of the room temperatures.
- Every 15 minutes a Bang-Bang controller operates the valves.

Case Study: Floor Heating System from Seluxit Aps

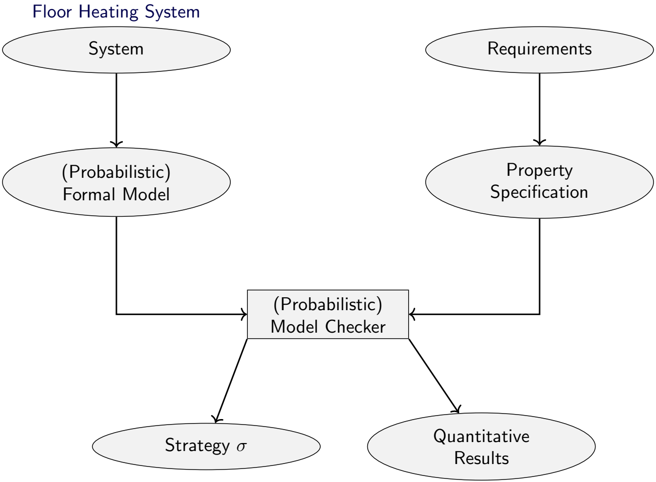
Requirement

Provide a controller which optimizes the comfort of the users.

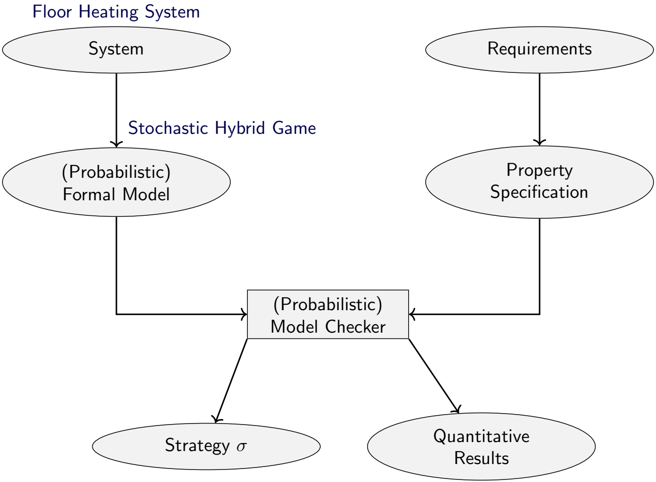
Near Optimal Strategy Synthesis



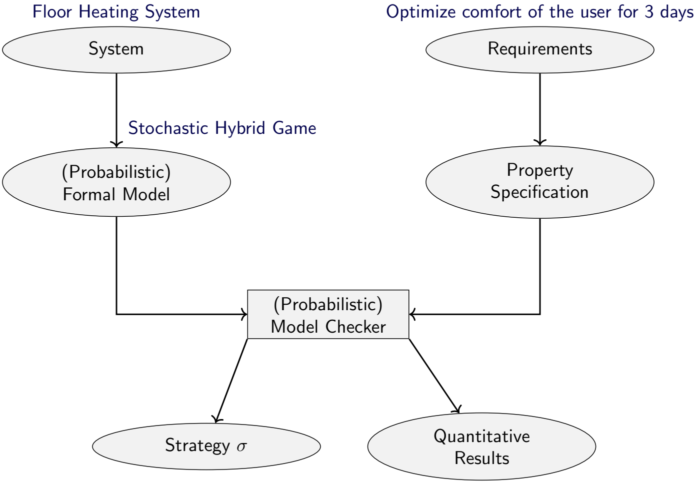
Near Optimal Strategy Synthesis



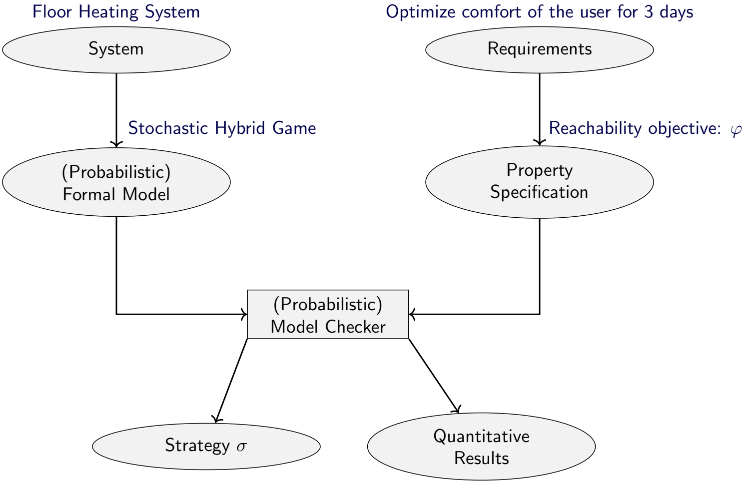
Near Optimal Strategy Synthesis



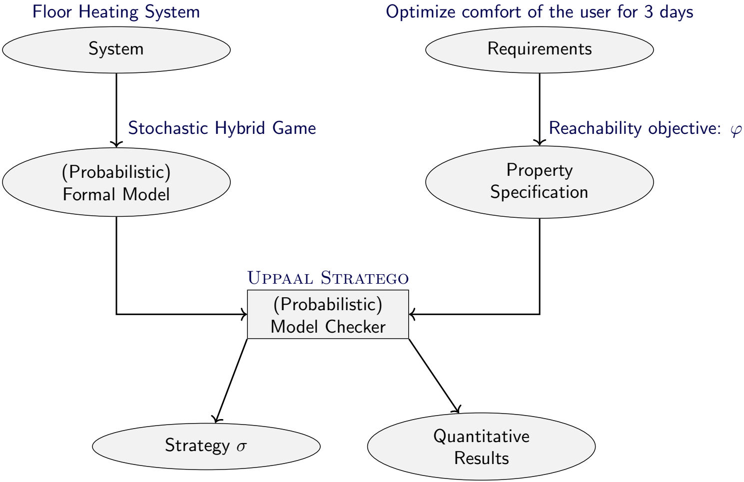
Near Optimal Strategy Synthesis



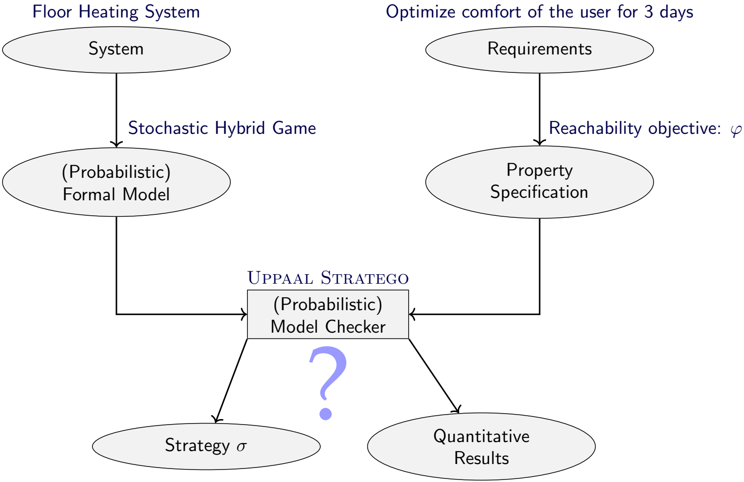
Near Optimal Strategy Synthesis



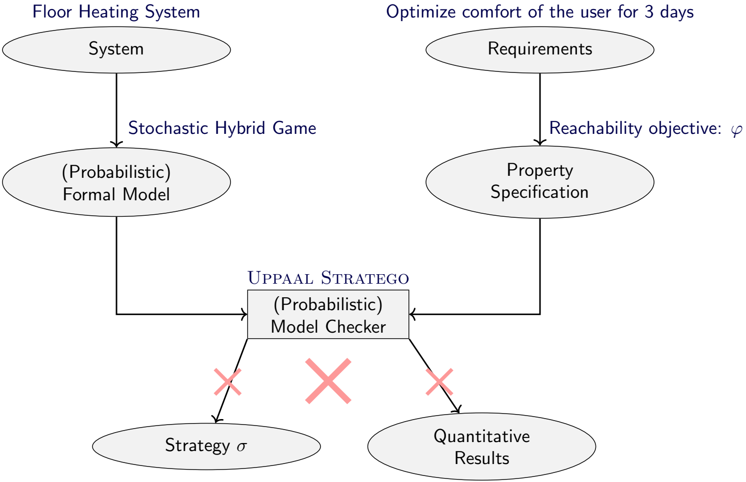
Near Optimal Strategy Synthesis



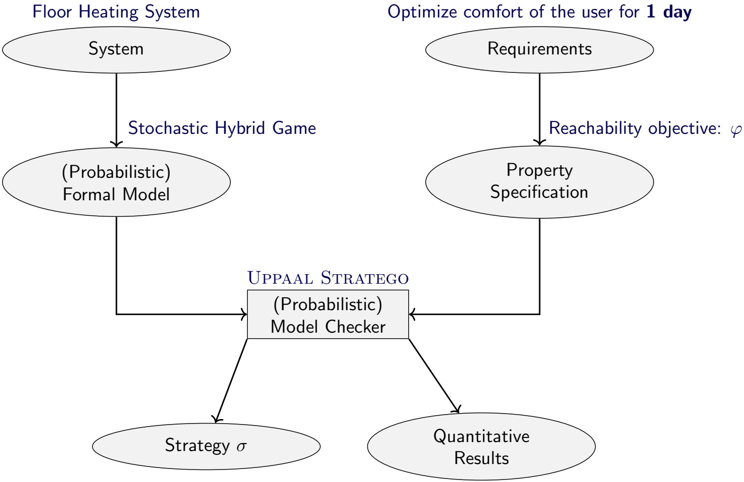
Near Optimal Strategy Synthesis



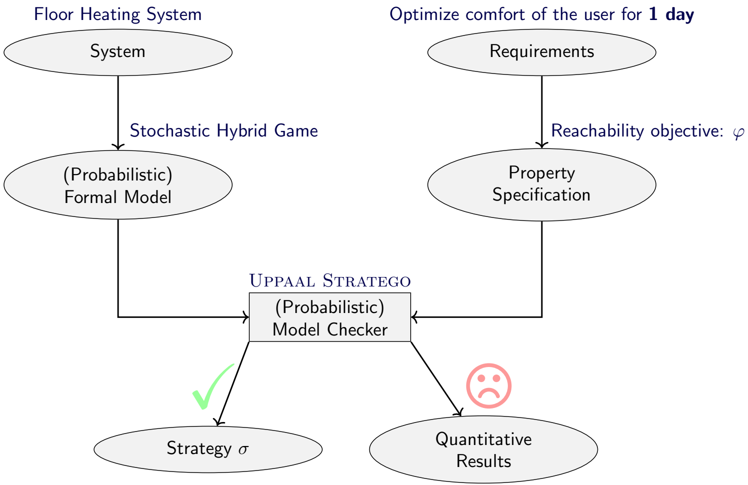
Near Optimal Strategy Synthesis



Near Optimal Strategy Synthesis



Near Optimal Strategy Synthesis



Stochastic Hybrid Game for CPS

A *stochastic hybrid game* is a tuple

$$\mathcal{G}_{n,m} = (\mathcal{C}, \mathcal{U}, X, \mathcal{F}, \delta)$$

where:

- $\mathcal{C}$ is a controller with controllable modes $C = \{c_1, \ldots, c_n\}$,
- $\mathcal{U}$ is the environment with uncontrollable modes $U = \{u_1, \ldots, u_m\}$,
- $X = \{x_1, \ldots, x_n\}$ is a finite set of continuous (real-valued) variables,
- $\mathcal{F}_{c,u} : \mathbb{R}_{>0} \times \mathbb{R}^X \rightarrow \mathbb{R}^X$ is the flow-function for each $c \in C$ and $u \in U$,
- δ is a family of density functions, indicating the switching among uncontrollable modes U.

Thermodynamics

The evolution of the room temperatures $\mathcal{F}_{v,d}$ are the solutions to the following differential equations:

$$\frac{d}{dt} T_i(t) = \sum_{j=1}^{n} A^d_{i,j}(T_j(t) - T_i(t)) + B_i(T_{\text{env}}(t) - T_i(t)) + H^v_{j,i} \cdot v_j$$

Where:

- A^d represents the heat exchange coefficients among the different rooms given the door configuration d,
- B represents the heat exchange coefficients between the environment and each room,
- H^v represents the heat exchange coefficients among each pipe and the rooms it heats given the valve configuration v,

Optimal Controlling

Given strategy σ^H, $\mathcal{G}_{n,m} \upharpoonright \sigma^H$ is a stochastic process.

Goal

Synthesize a near-optimal strategy σ^H which minimizes the expected value of a function

$$\sigma^H = \mathrm{argmin}_{\sigma} \mathbb{E}^{\mathcal{G}}_{\sigma,H}(f)$$

Optimal Controlling

Given strategy σ^H, $\mathcal{G}_{n,m} \upharpoonright \sigma^H$ is a stochastic process.

Goal

Synthesize a near-optimal strategy σ^H which minimizes the expected value of a function

$$\sigma^H = \mathrm{argmin}_\sigma \mathbb{E}^{\mathcal{G}}_{\sigma,H}(f)$$

Discomfort measure the integrated deviation of the current room temperatures wrt. the target temperatures.

$$f = \int_0^H \sum_i^n (T_i^g - T_i(t))^2 \cdot W_i \; dt$$

Online Synthesis

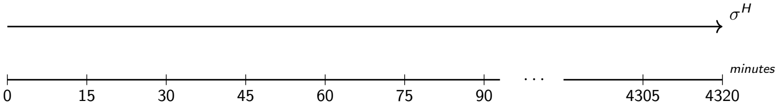
Periodically compute the controller only for the near future [LMM+16]

Online Synthesis

Periodically compute the controller only for the near future [LMM+16]

For n rooms, a Horizon H of 3 days and controlling every 15 min.

Compute a strategy σ^h for the next 45 min.

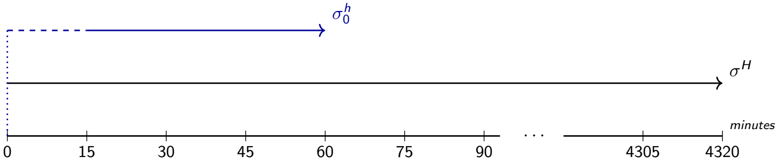


Online Synthesis

Periodically compute the controller only for the near future [LMM+16]

For n rooms, a Horizon H of 3 days and controlling every 15 min.

Compute a strategy σ^h for the next 45 min.

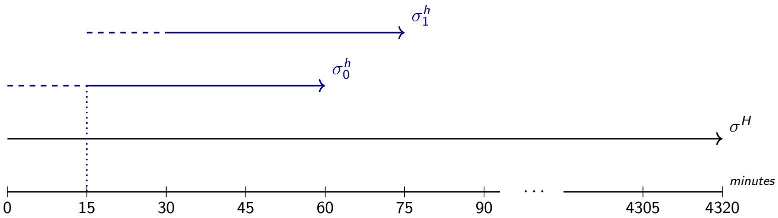


Online Synthesis

Periodically compute the controller only for the near future [LMM+16]

For n rooms, a Horizon H of 3 days and controlling every 15 min.

Compute a strategy σ^h for the next 45 min.

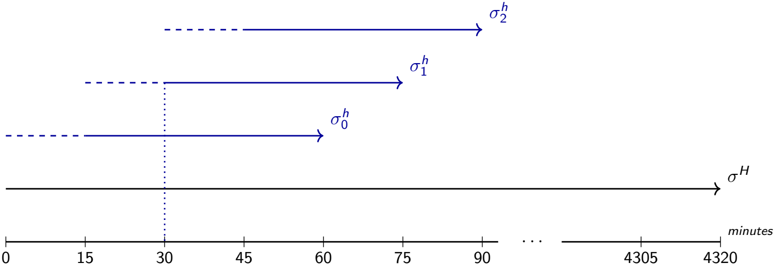


Online Synthesis

Periodically compute the controller only for the near future [LMM$^+$16]

For n rooms, a Horizon H of 3 days and controlling every 15 min.

Compute a strategy σ^h for the next 45 min.

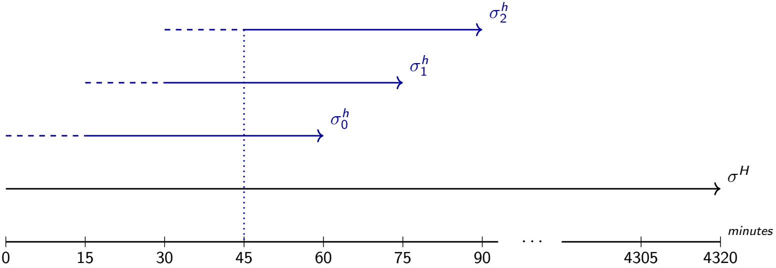


Online Synthesis

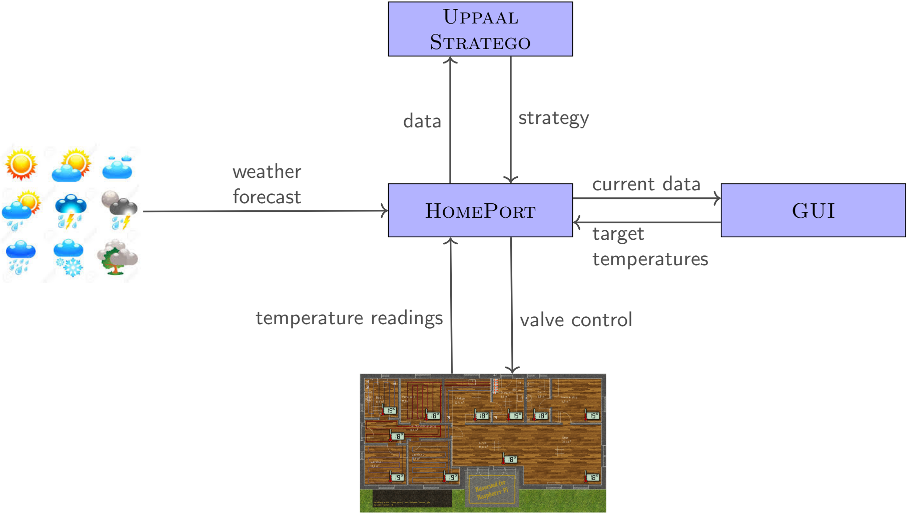
Periodically compute the controller only for the near future [LMM+16]

For n rooms, a Horizon H of 3 days and controlling every 15 min.

Compute a strategy σ^h for the next 45 min.



Floor Heating: Tool Chain Architecture

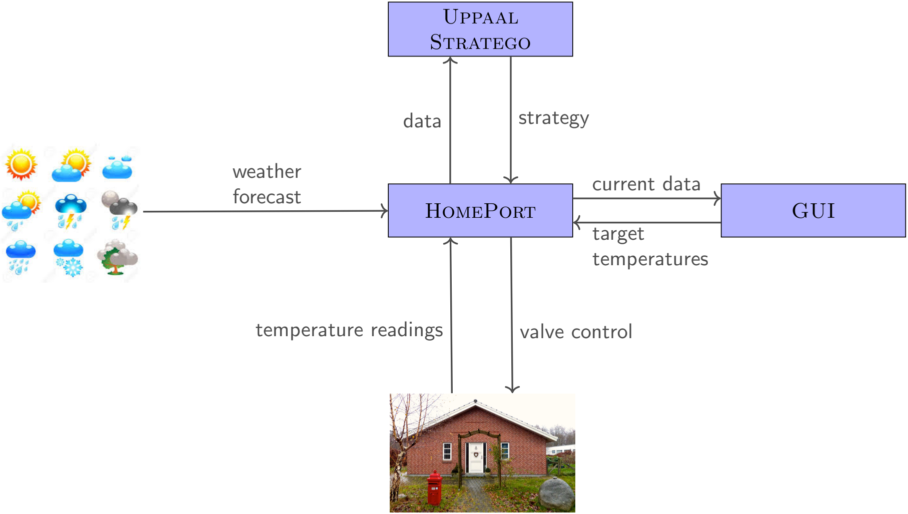


$$\frac{d}{dt}T_i(t) = \sum_{j=1}^{n} A^d_{i,j}(T_j(t) - T_i(t)) + B_i(T_{\text{env}}(t) - T_i(t)) + H^v_{j,i} \cdot v_j$$

Experimental Data - Three Day Scenarios

Weather	Discomfort			Energy		
	Bang-Bang	Stratego	imp.	Bang-Bang	Stratego	imp.
Aalborg	14583	8342	**43**%	14180	12626	**10**%
Anadyr	2385515	1483272	**37**%	23040	22475	**2**%
Ankara	17985	10464	**41**%	17468	15684	**10**%
Minneapolis	22052	12175	**44**%	18165	15882	**12**%
Murmansk	399421	187941	**52**%	22355	21011	**6**%

Floor Heating: Tool Chain Architecture



Thesis Proposal: Synthesis of Optimal Controllers for Hybrid Solar Water Heating Systems

Floor Heating

Solar Water Heating Systems

Thesis Proposal: Synthesis of Optimal Controllers for Hybrid Solar Water Heating Systems

Some tasks

- Propose Intelligent Hybrid Solar Water Heating Systems
- Formally model the proposed systems
- Formally specify sensitive requirements e.g. "hot water output is at least 300 liters".
- Synthesize near optimal strategies
- Compare the performance of the different systems

Solar Water Heating Systems

Bibliography I

Parosh Abdulla, Stavros Aronis, Bengt Jonsson, and Konstantinos Sagonas, *Comparing source sets and persistent sets for partial order reduction*, pp. 516–536, Springer International Publishing, Cham, 2017.

F.M. Boenneland, P.G. Jensen, K.G. Larsen, M. Muniz, and J. Srba, *Start pruning when time gets urgent: Partial order reduction for timed systems*, Proceedings of the 30th International Conference on Computer Aided Verification (CAV'18), LNCS, Springer-Verlag, 2018, To appear., pp. 1–19.

Johan Bengtsson, Bengt Jonsson, Johan Lilius, and Wang Yi, *Partial order reductions for timed systems*, CONCUR'98 Concurrency Theory (Berlin, Heidelberg) (Davide Sangiorgi and Robert de Simone, eds.), Springer Berlin Heidelberg, 1998, pp. 485–500.

Johan Bengtsson and Wang Yi, *Timed automata: Semantics, algorithms and tools*, Advances in Petri Nets, Springer-Verlag, 2004, pp. 87–124.

Patrice Godefroid, *Using partial orders to improve automatic verification methods*, Proceedings of the 2Nd International Workshop on Computer Aided Verification (Berlin, Heidelberg), CAV '90, Springer-Verlag, 1991, pp. 176–185.

Bibliography II

- Henri Hansen, Shang-Wei Lin, Yang Liu, Truong Khanh Nguyen, and Jun Sun, *Diamonds are a girl's best friend: Partial order reduction for timed automata with abstractions*, Computer Aided Verification (Cham) (Armin Biere and Roderick Bloem, eds.), Springer International Publishing, 2014, pp. 391–406.

- Richard J. Lipton, *Reduction: A method of proving properties of parallel programs*, Commun. ACM **18** (1975), no. 12, 717–721.

- K.G. Larsen, M. Mikucionis, M. Muniz, J. Srba, and J.H. Taankvist, *Online and compositional learning of controllers with application to floor heating*, Proceedings of the 22nd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'16), LNCS, vol. 9636, Springer-Verlag, 2016, pp. 244–259.

- Antoni Mazurkiewicz, *Trace theory*, Petri Nets: Applications and Relationships to Other Models of Concurrency (Berlin, Heidelberg) (W. Brauer, W. Reisig, and G. Rozenberg, eds.), Springer Berlin Heidelberg, 1987, pp. 278–324.

- Marius Minea, *Partial order reduction for model checking of timed automata*, Proceedings of the 10th International Conference on Concurrency Theory (London, UK, UK), CONCUR '99, Springer-Verlag, 1999, pp. 431–446.

Bibliography III

- Doron Peled, *All from one, one for all: on model checking using representatives*, Computer Aided Verification (Berlin, Heidelberg) (Costas Courcoubetis, ed.), Springer Berlin Heidelberg, 1993, pp. 409–423.
- Ramzi Ben Salah, Marius Bozga, and Oded Maler, *On interleaving in timed automata*, CONCUR 2006 – Concurrency Theory (Berlin, Heidelberg) (Christel Baier and Holger Hermanns, eds.), Springer Berlin Heidelberg, 2006, pp. 465–476.
- Antti Valmari, *Stubborn sets for reduced state space generation*, Advances in Petri Nets 1990 (Berlin, Heidelberg) (Grzegorz Rozenberg, ed.), Springer Berlin Heidelberg, 1991, pp. 491–515.