Benchmarks for cyber-physical systems: A modular model library for building automation systems (Extended version)

Nathalie Cauchi, Alessandro Abate
Department of Computer Science, University of Oxford, Oxford, U.K
name.surname@cs.ox.ac.uk

Abstract

Building Automation Systems (BAS) are exemplars of Cyber-Physical Systems (CPS), incorporating digital control architectures over underlying continuous physical processes. We provide a modular model library for BAS drawn from expertise developed on a real BAS setup. The library allows to build models comprising of either physical quantities or digital control modules.The structure, operation, and dynamics of the model can be complex, incorporating (i) stochasticity, (ii) non-linearities, (iii) numerous continuous variables or discrete states, (iv) various input and output signals, and (v) a large number of possible discrete configurations. The modular composition of BAS components can generate useful CPS benchmarks. We display this use by means of three realistic case studies, where corresponding models are built and engaged with different analysis goals. The benchmarks, the model library and data collected from the BAS setup at the University of Oxford, are kept on-line at `https://github.com/natchi92/BASBenchmarks`.

Keywords 1 *cyber-physical systems, building automation systems, thermal modelling, hybrid models, simulation, reachability analysis, probabilistic safety, control synthesis*

1 Introduction

This paper describes a library of models for Building Automation Systems (BAS), which can be employed to create benchmarks for verification, control synthesis, or simulation purposes of Cyber-Physical Systems (CPS). The models are inspired by and built around an experimental setup within the Department of Computer Science at the University of Oxford, which is part of on-going research in collaboration with service engineers and industrial partners in the sector. This library allows to create numerous meaningful models for BAS, which are examples of CPS integrating continuous dynamics and discrete modes.

Interest in BAS, also colloquially known as *smart buildings*, is gaining rapid momentum, in particular as a means for ensuring thermal comfort ([1]), minimising energy consumption ([16, 18]), and ascertaining reliability ([3, 19]). Quantitative models are needed to

evaluate system performance, to verify correct behaviour, and to develop specific control algorithms. An overview of the different BAS modelling techniques used in literature is presented in [15]. Several simulation tools (see [5]) have been devised to aide in the development and analysis of models for BAS. Attempting a multi-dimensional characterisation of the broad spectrum of existing BAS models, we can find either deterministic or stochastic ones, low- to high-dimensional ones, with discrete or continuous inputs and states. The choice of a model is an art and a craft ([14]): one must select simplifying assumptions that accurately reflect the operational performance of the BAS in specific real-world environments, and introduce uncertainty to represent un-modelled components, unknown parameters or random occupants. We therefore aim to simplify the modelling process such that simulation, verification or strategy synthesis can be carried out seamlessly. Different verification and policy synthesis tools exist in literature ([6, 10, 11]). They are typically specific to a particular type of model structure and in the case of stochastic or hybrid models are oftenlimited to a small number of continuous variables. The use of such tools also requires expert knowledge on the specific formalism the tool makes use of.

In order to display the versatility of the library of BAS models, we present three case studies that are built from its components. We focus on modelling temperature dynamics, a key element for ensuring thermal comfort. We employ the three generated models for different analysis goals, comprising simulation, reachability, and control synthesis. The models and delineation of the case-studies are kept on-line at

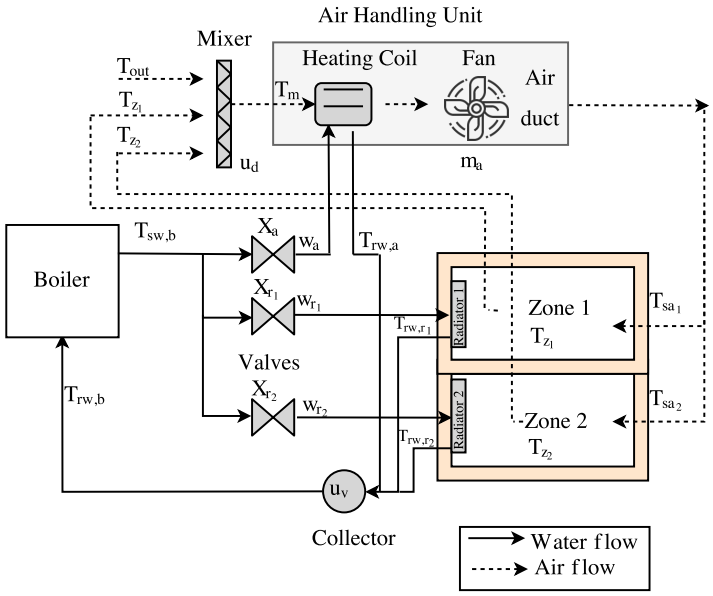
`https://github.com/natchi92/BASBenchmarks`.

This is to allow their use or modification for different applications and for comparison with other modelling approaches in BAS. The repository also contains real data gathered from the BAS lab at Oxford, which can be employed for further modelling studies. This article has the following structure: Section 2 introduces the BAS modelling framework for CPS. We identify three modelling trade-offs that introduce different complexities on the model dynamics. Based on these trade-offs, we develop and analyse three case studies in Section 3.

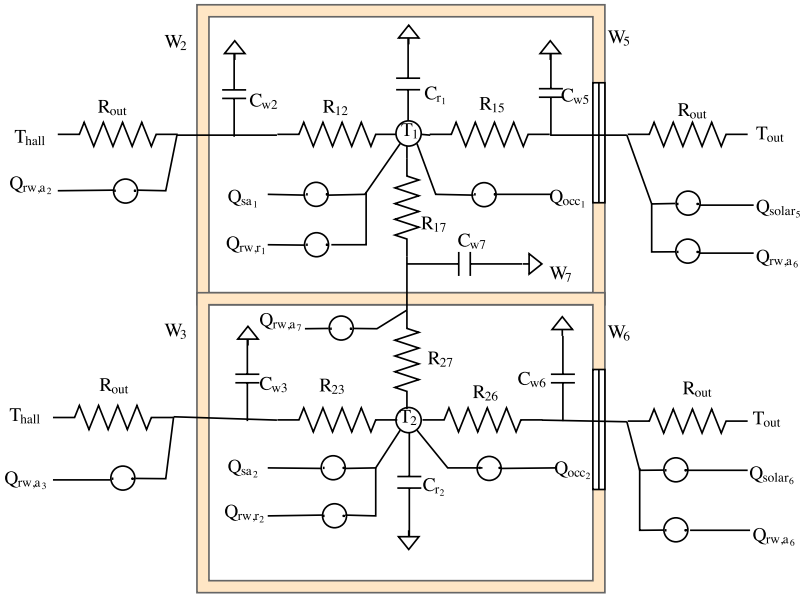
2 Building Automation Systems

2.1 BAS: structure and components

BAS models clearly depend on the size and topology of the building ([12]), and on its climate control setup. In this work, we consider the BAS setup in the Department of Computer Science, at the University of Oxford. A graphical depiction is shown in Figure 1a. The BAS consists of two teaching rooms that are connected to a boiler-heated system. The boiler supplies heat to the heating coil within the AHU and to two radiators. Valves control the rate of water flow in the heating coil and in radiators. The AHU supplies air to the two zones, which are connected back to back, and adjacent both to the outside and to an interior hall (cf. Figure 1a). The zone air of both rooms can mix with the outside air and exchanges circulating air with the AHU. Return water from the AHU heating coils and radiators is collected and pumped back to the boiler. Figure 1b presents the Resistor Capacitance (RC) network circuit of the two zones ([8]), which underpins the dynamics for temperature in the zone component - corresponding equations are in Table 3. The heat level in each room is modified by (i) radiative solar energy absorbed through the walls, (ii) occupants, (iii) AHU input supply air, (iv) radiators, and (v) AHU return water. The effect of heat stored in the walls and in rooms is depicted with capacitors, whereas thermal resistance to heat transfer by the walls is depicted by resistor elements.



(a) 2-zone boiler-based heating system with air handling unit and radiators



(b) Resistance-capacitance circuit for the internal thermal dynamics within the two zones

Figure 1: Building automation system setup

2.2 BAS: dynamics and configurations

We define models for the individual components in the BAS system based on the expertise developed on the BAS setup at Oxford. Single components are intended as separate physical structures within the BAS. Their models are built from the underlying physics and are improved via industrial feedback and from existing literature ([8]). We obtain models with a number of unknown parameters: these are estimated and validated using data collected from the BAS setup [13]. We list indices in Table 1, while all the quantities (variables, parameters, inputs) are listed in Table 2. Table 3 presents all the relations among variables in the model: algebraic relations define static couplings, whereas differential relations define the dynamics for the corresponding variables. The structure in Figure 1a, the quantities in Table 2, and the variables (with associated dynamics) in Table 3, together allow to construct global models for the complete BAS setup. We refer to the set of models describing the individual components (cf. Table 3) as a library of models: one can select the individual components and models from the library, and build different BAS configurations.

Table 1: Indices

Index	**Reference**	**Index**	**Reference**
a	AHU	adj	adjacent zone
adj, out	adjacent exterior zones	b	boiler
d	mixer	$hall$	hallway
$i = \{1, 2\}$	individual zones	$jn = \{2, 3, 7\}$	zone walls with no windows
$jw = \{5, 6\}$	zone walls with windows	$j = jn \cup jw$	all zone walls
$l \in \{1, 2\}$	adjacent interior zone	occ	occupants
out	outside	r	radiator
ref	reference	rw	return water
sa	supply air	$solar$	solar energy
sw	supply water	v	collector
w	wall	z	zone
h	water	ar	air

A global model of the BAS set-up can be complex, comprising both algebraic and differential relations that may be further affected by process noise. A model also contains a number of inputs which can either be construed as control signals or as exogenous signals. Some of the dynamics are non-linear in view of continuous variables that are bi-linearly coupled (cf. AHU air duct model in Table 3). The number of continuous variables also increase substantially when considering a BAS setup with multiple zones: employing the zone component for a configuration with n zones would result in a model with $(2n + 1) + n$ continuous state variables. Furthermore, the model features multiple components that present switching discrete behaviours, affecting the dynamics of the continuous variables: these discrete modes are listed in Table 4 and can result in up to 144 discrete configurations.

In order to tackle the complexity of global BAS models and to add a level of flexibility to the modelling framework, we consider each BAS component as a separate module, characterised by inputs and output elements, and internal variables. We make use of individual modules describing component type, and then connect different modules based on possible physical couplings. Coupling between different modules is also achieved via input-output relationships: e.g., in the zone module we have coupling between two zones through the continuous variable $T_{adj,l}$ corresponding to the adjacent zones, which for the wall separating the two zones (cf. W_7 in Figure 1b) corresponds to the individual zone temperatures of the two zone modules (cf. Table 3 zone equations). Having such a modular structure for the individual components provides an added level of versatility, since we can connect different components to create various new models. Modularisation also allows (i) to perform analysis of the whole setup by executing analysis of individual modules and (ii) to extend the library of models by defining new modules that connect to existing modules via their input-output relations.

Symbol	Quantity	Type
A_i	area of windows of each zone	constant
B_{en}	boiler switched off	discrete
C	capacitance of medium	constant
C_{pa}, C_{pw}	specific heat capacity of air and water	constant
CO_{2_i}	carbon-dioxide measurements in each zone	input
k_b	steady-state of the boiler	constant
m	mass air flow rate	input
n	number of zones	constant
P_{out}	radiator rated power output	constant\input
Q	associated heat gain	input
R	thermal resistance to heat from walls to medium	constant
T	temperature of associated medium	state\input
u	mixing ratio	input
(UA)	overall transmittance factor of medium	constant
V	volume of medium	constant
w	water flow rate of associated medium	input
w_{max}	maximum water-flow permitted by the valve	constant
X	valve position of associated component	input
$\{\alpha, \beta, \mu\}$	de-rating and offset factors	constants
σ	the associated process noise	constant
ρ	density of medium	constant
τ	time constant of the medium	constant

Table 2: List of variables, inputs, and parameters

2.3 BAS: description of model library

The library of BAS components comes in the form of MATLAB scripts. Each script represents an individual BAS component. The models are in state-space form and are of two types linear or bilinear depending on the component they represent. They are defined using the symbolic toolbox, are parametrised and can be described both in discrete and continuous time. We provide the parameters which we estimated from data gathered from the BAS lab to construct the individual models. However, users can easily make use of their own parameters and construct their own model. Different components can be connected together based on their input-output relations by cascading the different symbolic models for each component. Once this is done, the provided scripts allow you to simulate the models and plots for the defined output variables are presented.

3 Case studies

Next we set up three case studies and present the trade off between the discussed elements of complexity. For each of the case studies, we (i) establish the dynamics of the models, (ii) how they are constructed from the library of components and (iii) and describe the results obtained

3.1 Two-zone heating setup with deterministic or stochastic dynamics

We consider two zones, each heated by one radiator and with a common supply air, as portrayed in Figure 2. From Table 3, we select two components and corresponding models: the

Component: Boiler	
Continuous variables	**Relation**
$dT_{sw,b}(t) = \begin{cases} 0 & B_{en}(t) = 0 \\ (\tau_{sw})^{-1}\left[(-T_{sw,b}(t) + k_b)dt\right] + \sigma_{sw}dW & B_{en}(t) = 1 \end{cases}$	differential
Component: Valve	
Continuous variables	**Relation**
$w(t) = (\tau)^{-1}\left[\exp(\ln(\tau)X(t))w_{max}\right]$	algebraic
Component: Mixer	
Continuous variables	**Relation**
$T_d(t) = u_d T_{out}(t) + (1-u_d)(\sum_i T_{z_i}(t))(n)^{-1}$	algebraic
Component: AHU heating coil	
Continuous variables	**Relation**
$dT_{rw,a}(t) = (C_{pw}\rho_h V_a)^{-1}\left[(C_{pw}w_a(t)(T_{sw,b}(t) - T_{rw,a}(t)) + (UA)_a(T_d(t) - T_{rw,a}(t)))dt\right] + \sigma_{rw,a}dW$	differential
Component: AHU air duct	
Continuous variables	**Relation**
$dT_{sa_i}(t) = (C_a\rho_a V_a)^{-1}\left[m_a(t)C_{pa}(T_d(t) - T_{sa_i}(t)) + (UA)_a(T_{z_i}(t) - T_{sa_i}(t))\right]dt + \sigma_{sa_i}dW$	differential
Component: Radiator	
Continuous variables	**Relation**
$dT_{rw,r_i}(t) = (C_{pw}\rho_h V_{r_i})^{-1}\left[(C_{pw}w_{r_i}(t)(T_{sw,b}(t) - T_{rw,r_i}(t)) + (UA)_{r_i}(T_{z_i}(t) - T_{rw,r_i}(t)))dt\right] + \sigma_{rw,r_i}dW$	differential
Component: Zone	
Continuous variables	**Relation**
$dT_{z_i}(t) = (C_{z_i})^{-1}\left[\frac{T_{w_{j_n}}(t) - T_{z_i}(t)}{R_{ij}} + Q_{rw,r_i}(t) + Q_{occ_i}(t) + Q_{sa_i}(t)\right]dt + \sigma_{z_i}dW$	differential
$dT_{w_{j_n}}(t) = \left(C_{w_{j_n}}\right)^{-1}\left[\frac{T_{adj,out}(t) - T_{z_i}(t)}{R_{out}} + \sum_l \frac{T_{adj_l}(t) - T_{w_{j_n}}(t)}{R_{lj}} + Q_{rw,a_{j_n}}(t)\right]dt + \sigma_{w_{j_n}}dW$	
$dT_{w_{j_w}}(t) = \left(C_{w_{j_w}}\right)^{-1}\left[\frac{T_{adj,out}(t) - T_{z_i}(t)}{R_{out}} + \sum_l \frac{T_{adj_l}(t) - T_{w_{j_w}}(t)}{R_{ljw}} + Q_{solar_{j_w}}(t) + Q_{rw,a_{j_w}}(t)\right]dt + \sigma_{w_{j_w}}dW$	
$Q_{rw,r_i}(t) = P_{rad_i}(\alpha_2(T_{rw,r_i}(t) - T_{z_i}(t)) + \alpha_1), Q_{occ_i}(t) = \mu_i(CO_{2_i}(t)) + \beta_{1_i}, Q_{sa_i}(t) = m_a(t)C_{pa}(T_{sa_i}(t) - T_{z_i}(t)))$	
$Q_{rw,a_j}(t) = \alpha_3(T_{rw,a}(t) - T_{w_j}(t)), Q_{solar_{j_w}}(t) = (\alpha_0 A_i T_{out}(t) + \beta_2)$	
Component: Collector	
Continuous variables	**Relation**
$T_{rw,b}(t) = u_v T_{rw,a}(t) + (1-u_v)(\sum_i T_{rw,r_i}(t))(n)^{-1}$	algebraic

Table 3: Components dynamics and functional relations among variables

Component	**Discrete Modes**
Boiler	Boiler on, off (B_{en})
AHU air duct	Fan off, medium, high (m_a)
Mixer	Open, closed (u_d)
AHU heating coil	Valve healthy, faulty (X_a)
Radiator heating coil 1	Valve healthy, faulty (X_{r_1})
Radiator heating coil 1	Valve fully open, half open, closed (X_{r_1})

Table 4: Discrete operational modes

radiator and the zone. We simplify these models with the following assumptions: (i) the wall temperature is constant across the zones and is a fixed value ($T_{w,ss}$); (ii) the boiler is switched ON providing a supply temperature $T_{sw,b_{ss}}$; (iii) we fix both the mass air flow rate m_a and the radiator water flow rate w_r; and (iv) we do not include the heat gain from the windows and the AHU heating coils ($T_{w_{ss}}$) in each zone. We obtain a model with the four state variables $x^T = \begin{bmatrix} T_{z_1} & T_{z_2} & T_{rw,r_1} & T_{rw,r_2} \end{bmatrix}^T$ and with a common supply temperature $u = T_{sa}$ as an input. For this setup we further consider three different dynamics: (i) a purely

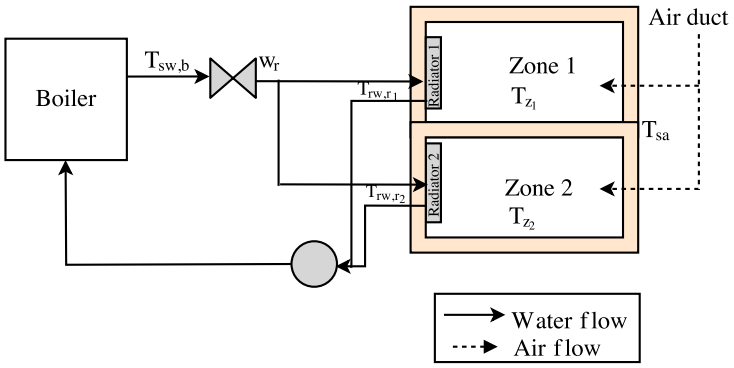


Figure 2: BAS setup for the first case study

deterministic one; (ii) a deterministic model with additive disturbance; and (iii) a stochastic model. For (i) and (ii), we thus remove the process noise in the template model, while for models (i) and (iii) we do not include the occupancy heat gain. We also discretise the dynamics by a Forward-Euler scheme (for the deterministic models) and a Euler-Maruyama scheme (for the stochastic model), using a uniform sampling time $\Delta = 15$ minutes, and obtain a set of linear discrete-time models. One should note that the models being considered are not fully observable since for all the individual zone temperatures (variables of interest) are the only variables provided as outputs. The dynamics of the deterministic model (i) are described by

$$\mathbf{M}_d : \begin{cases} x[k+1] & = Ax[k] + Bu[k] + Q_d \\ y_d[k] & = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} x[k], \end{cases} \tag{1}$$

where again the matrices are properly sized and constructed based on the models in Table 3 and where,

$$Q_d = \begin{bmatrix} \frac{T_{w_{ss}}\Delta}{C_{z_1}R_1} & \frac{T_{w_{ss}}\Delta}{C_{z_2}R_2} & \frac{C_{pw}w_{r_1}\Delta}{C_{pw}\rho_h V_{r_1,b}}T_{sw,b_{ss}} & \frac{C_{pw}w_{r_2}\Delta}{C_{pw}\rho_h V_{r_2,b}}T_{sw,b_{ss}} \end{bmatrix}^T$$

Here R_i is the mean resistance offered by the walls. The deterministic model with additive disturbances is

$$\mathbf{M}_{da} : \begin{cases} x[k+1] & = Ax[k] + Bu[k] + F_{da}d_{da}[k] \\ & \quad + Q_{da} \\ y_{da}[k] & = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} x[k]. \end{cases} \tag{2}$$

We have extended (1) with additive noise vector $d_{da}^T = \begin{bmatrix} CO_{2_1} & CO_{2_2} \end{bmatrix}^T$ (cf. Q_{occ_i} in Table 3) representing the different CO_2 levels in each zone. Q_{da} is defined as $Q_{da} = Q_d + \begin{bmatrix} \frac{\beta_{1_1}\Delta}{C_{z_1}} & \frac{\beta_{1_2}\Delta}{C_{z_2}} & 0 & 0 \end{bmatrix}^T$ and F_{da} is a properly sized matrix.The stochastic model is expressed by extending (1) to include process noise, as

$$\mathbf{M}_s : \begin{cases} x[k+1] & = Ax[k] + Bu[k] + Q_d + \Sigma W[k] \\ y_s[k] & = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} x[k], \end{cases} \tag{3}$$

where $\Sigma = diag([(\sqrt{\Delta}\sigma_{z_1})^2 \ (\sqrt{\Delta}\sigma_{z_2})^2 \ (\sqrt{\Delta}\sigma_{rw,r_1})^2 \ (\sqrt{\Delta}\sigma_{rw,r_2})^2])$encompasses the variances of the process noise for each state. $W = \begin{bmatrix} w_1 & w_2 & w_3 & w_4 \end{bmatrix}^T$ are independent Gaussian random variables, which are also independent of the initial condition of the process. A simulation run of all three models is depicted in Figure 3.

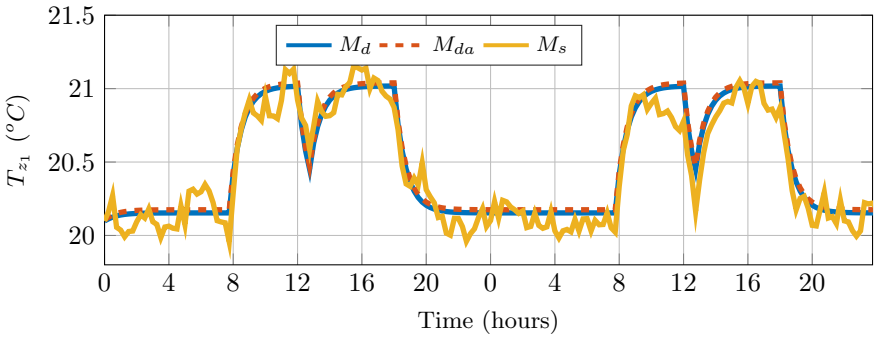


Figure 3: First case study: simulations over two days

3.1.1 Reachability analysis

For this case study we would like to perform the following verification task: to decide whether traces generated by the models remain within a specified safe set for a given time period. This is achieved by reachability analysis, which takes a probabilistic flavour for the stochastic model. The safe set is described as an interval around the temperature set-point $T_{SP} = 20^oC$ $\pm 0.5^oC$. We constrain the input u to lie within the set $\{T_{sa} \in \mathbb{R} | 15 \leq T_{sa} \leq 22\}$ for all models and employ a fixed time horizon $N = 6 \times \Delta = 1.5$ hours. We perform reachability analysis with Axelerator ([2]), while we use FAUST^2 ([17]) to perform probabilistic reachability analysis of $\mathbf{M}_s$.

In order to perform reachability analysis using Axelerator, for each of the models we set the initial condition as $\begin{bmatrix} T_{z_1} & T_{z_2} & T_{rw,r_1} & T_{rw,r_2} \end{bmatrix}^T = \begin{bmatrix} 18 & 18 & 35 & 35 \end{bmatrix}^T$. The reach tube for model $\mathbf{M}_d$ over the whole time horizon is shown in Figure 4: it encompasses the union of reachable states over that horizon. The results obtained using Axelerator (cf. Figure 4) are conservative results and confirm that the model can indeed stay in the required safe set for some initial states, but can also exit it.One can note the coupling between the two zones and that zone 1 tends to stay at higher zone temperatures then zone 2. A similar reach tube is obtained for model $\mathbf{M}_{da}$.

Similarly, we perform probabilistic reachability analysis on model $\mathbf{M}_s$ by defining the same safe set and assuming an input set of [15 22]. The resulting adaptive partition of the safe set along with the optimal safety probability for each partition set is depicted in Figure 5. When performing probabilistic reachability analysis using model $\mathbf{M}_s$ (cf. Figure 5), we deduce that the models have a high probability of being within the required safe set, specifically to have $T_{z_1} \in [19.5\ 20]$ and $T_{z_2} \in [19.5\ 20.5]$.

3.2 Two-zone heating setup with large number of continuous variables

In this second case study we focus on the dynamics of the zone component from Table 3 and consider the two zones shown in Figure 1b. We assume that (i) a central fan pumps in air in both rooms with a common supply temperature $15^oC \leq T_{sa} \leq 30^oC$, (ii) the input mass airflow m_a is fixed to 10 $m^3/hour$ and (iii) the return water temperature of the AHU heating coils is fixed ($T_{rw,a_{ss}} = 35^oC$). As in the previous case study, the selected model is discretised using Forward-Euler, with a sampling time $\Delta = 15$ minutes, to obtain the discrete-time model

$$\mathbf{M}_c : \begin{cases} x_c[k+1] & = A_c x_c[k] + B_c u_c[k] + F_c d_c[k] + Q_c \\ y_c[k] & = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} x_c[k]. \end{cases} \tag{4}$$

Here the variables are

$$x_c = \begin{bmatrix} T_{z_1} & T_{z_2} & T_{w_5} & T_{w_6} & T_{w_2} & T_{w_3} & T_{w_7} \end{bmatrix}^T,$$

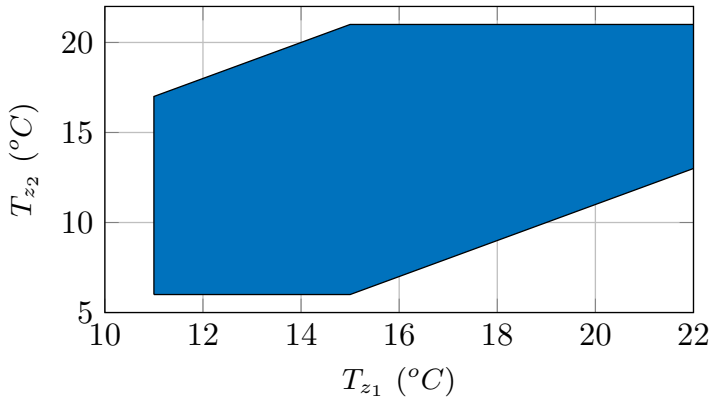


Figure 4: First case study: reach tube of M_d over whole time horizon

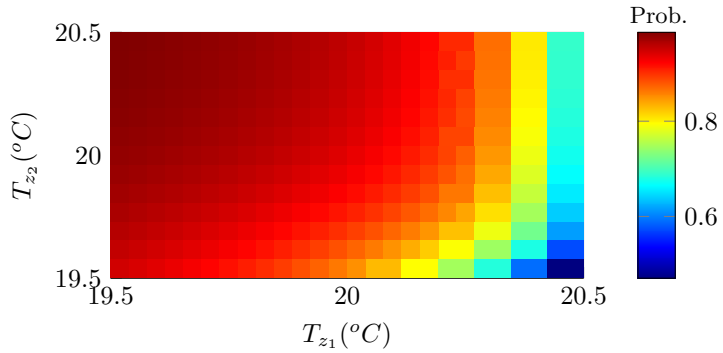


Figure 5: First case study: partition of the safe set for model M_s, along with optimal safety probability for each partition set

and a common fan supplies the two zones with a supply rate $u_c = T_{sa}$, whereas

$$d_c = \begin{bmatrix} T_{out} & T_{hall} & CO_{2_1} & CO_{2_2} & T_{rw,r_1} & T_{rw,r_2} \end{bmatrix}^T,$$

and

$$Q_c = \begin{bmatrix} \frac{q_{c_0}\Delta}{C_{z_1}} & \frac{q_{c_0}\Delta}{C_{z_2}} & \frac{q_{c_2}\Delta}{C_{w_5}} & \frac{q_{c_2}\Delta}{C_{w_6}} & \frac{q_{c_1}\Delta}{C_{w_2}} & \frac{q_{c_1}\Delta}{C_{w_3}} & \frac{q_{c_1}\Delta}{C_{w_7}} \end{bmatrix}^T,$$

where $q_{c_0} = \beta_{1_i} + \alpha_1 P_{rad_i}$, $q_{c_1} = \alpha_3 T_{rw,a_{ss}}$ and $q_{c_2} = \alpha_0 A_2 \beta_2 + q_{c_1}$. Matrices A_c, B_c, F_c are properly sized. Recall that the vector d_c corresponds to the disturbance signals, while Q_c represents constant additive terms within the model. We finally model the disturbances as random external effects.

3.2.1 Policy synthesis and refinement

For $\mathbf{M}_c$ we would like to synthesise a policy ensuring that the temperature within zone 1 does not deviate from the set point by more then 0.5^oC over a time horizon equal to four hours (i.e $N = 16$). This requirement can be translated into the following PCTL property

$\Phi := \mathbb{P}_{=p}[\Box^{\leq N=16}|T_{z_1} - T_{SP}| \leq 0.5]$. We then aim at synthesising a policy maximising the safety probability p. This synthesis goal can be computationally hard due to the number of continuous variables making up $\mathbf{M}_c$. To mitigate this limitation, we perform policy synthesis via abstractions ([9]). We simplify (4) into four abstract models using the technique in ([8]). The abstract models are labelled as $\mathbf{M}_{c_{a=\{4,\dots,1\}}}$, where a represents the number of continuous variables of the corresponding abstract model. The models take the form of Markov decision processes ([8]). We can quantify the error in the output variable, which has been introduced by the different levels of abstractions, through the use of (ε, δ)-*approximate simulation relations* ([9]). The pair (ε, δ) represents the deviation in the output trajectories between complex and abstract models and the differences in probability distribution of the processes, respectively. Such metrics allows the designer to select which of the considered abstract models provides the best trade off in precision: it is desirable to achieve little deviation in both the output trajectories (small ε) and in the probability distributions (small δ).

δ	1	$10^{\frac{-1}{2}}$	10^{-1}	$10^{\frac{-3}{2}}$	10^{-2}	$10^{\frac{-5}{2}}$	10^{-3}
$\mathbf{M}_{c_4}$	0.0008	0.1754	0.2084	0.2339	0.2555	0.2745	0.2910
$\mathbf{M}_{c_3}$	0.0006	0.1933	0.2312	0.2598	0.2831	0.3065	0.3241
$\mathbf{M}_{c_2}$	0.0011	0.1950	0.2373	0.2681	0.2928	0.3155	0.3278
$\mathbf{M}_{c_1}$	0.0010	0.1953	0.2371	0.2595	<u>0.2854</u>	0.3103	0.3254

Table 5: Second case study: error metrics (ε, δ) for concrete and abstract models.

We compute (ε, δ)-approximate simulation relations between $\mathbf{M}_c$ and the set of abstract models $\mathbf{M}_{c_{a=\{4,\dots,1\}}}$, as presented in Table 5. The (ε, δ) pair providing the optimal trade off is obtained with the abstract model $\mathbf{M}_{c_1}$ and corresponds to (0.2854, 10^{-2}). Next, we use FAUST^2 to perform a grid-based computation of the safety probability for $\mathbf{M}_{c_1}$ and obtain a model of size 14893 with an overall accuracy of 0.005. Over this approximation we synthesise the optimal policy for the abstract model which results in a safety probability of $p' = 0.9257$. We refine the obtained policy ([8]), which results in one that can be used with $\mathbf{M}_c$. The overall process results in Φ being satisfied with a safety probability of $p = p' - \eta - N\delta = 0.7657$, where η is the abstraction error introduced by FAUST^2. The results obtained further highlight that by trading off the complexity in the number of continuous variables and computing (ε, δ)-simulation relations, we can synthesise policies using simpler models, yet achieve high performance still when the refined policy is applied to the original model.

3.3 Single zone heating with multiple switching controls

In this third and last case study, we focus on mixer, AHU air duct, and zone components from Table 3. We select the AHU as the only source of heat within the zone (the boiler is disconnected). A pictorial description of this setup is in Figure 6. The mixer operates in either of two modes: open (Op) or closed (Cl). The AHU air duct recirculates air from either the internal zone (when $u_d = 0$ and the mixer is in mode Op) or from the outside (when $u_d = 1$ and the mixer is in mode Cl) via the continuous variable T_d (output of the mixer component). The rate of air being pumped into the zone (m_a) is controlled by the fan, which has three operating speeds (off O, medium M, and high H). The mixer position and the fan settings can be used to maintain a comfortable temperature within the zone. This setup can be described by a hybrid model. The discrete modes q are in the set $\{(O, -), (M, Op), (M, Cl), (H, Op), (H, Cl)\}$, and describe the possible configurations of fan operating speeds $\{O, M, H\}$ and mixer position $\{Op, Cl\}$. (When the fan is switched off, the mixer can be in any position as no air is pumped into the zone.) Continuous variables model the zone temperature (T_{z_1}) together with the supply air temperature (T_{sa}) being pumped into the zone. Transitions between discrete modes are triggered by continuous dynamics crossing spatial guards: guards denote deviations from temperature set-point as δ, $\delta_k, k = \{2, \dots, 5\}$, $\delta < \delta_2 < \delta_3 < \delta_4 < \delta_5$. A graphical description

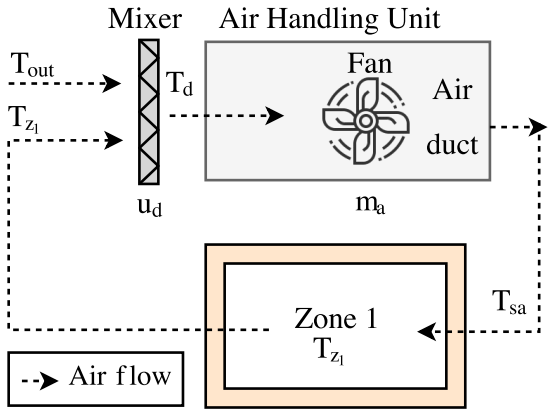


Figure 6: BAS setup for third case study

of the overall hybrid model, together with the different guard conditions, is shown in Figure 7. The continuous dynamics are built from Table 3 and follow

$$\dot{T}_{z_1} = (C_{z_1})^{-1}\,[\frac{T_{w_{ss}} - T_{z_1}(t)}{R} + m_a(t)C_{pa}(T_{sa}(t) - T_{z_1}(t) + \mu_1 CO2_{1_{ss}} + \beta_{1_1}],$$
$$\dot{T}_{sa} = (C_a\rho_a V_a)^{-1}\,[m_a(t)C_{pa}(T_d(t) - T_{sa}(t)) + (UA)_a(T_{z_1}(t) - T_{sa}(t)].$$

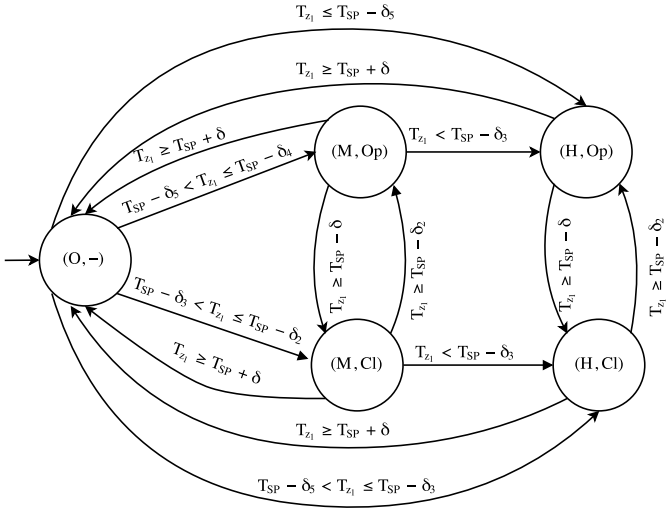


Figure 7: Hybrid model for the third case study, showing discrete states and guard conditions; the initial discrete state is $(O, -)$

The variables m_a and T_d take values according to the discrete mode as

$$m_a(t) = \begin{cases} 0 & q(t) = (O, -), \\ m_{a,med} & q(t) = (M, Op) \vee q(t) = (M, Cl), \\ m_{a,high} & q(t) = (H, Op) \vee q(t) = (H, Cl), \end{cases}$$

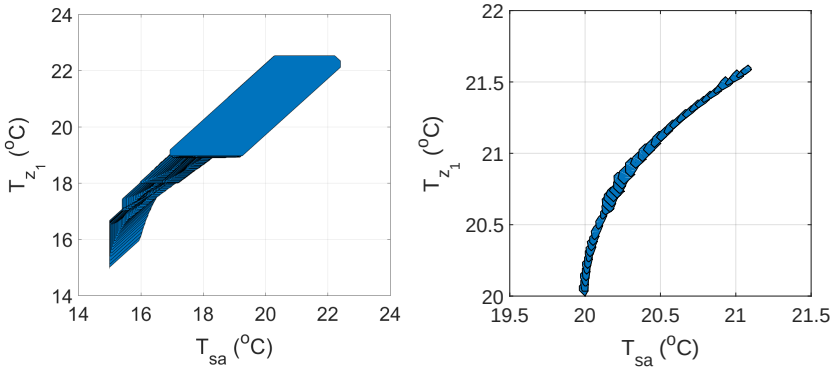
and

$$T_d(t) = \begin{cases} T_{out} & q(t) = (M, Op) \vee q(t) = (H, Op), \\ T_{z_1}(t) & \text{else.} \end{cases}$$

Here, $m_{a,med}, m_{a,high}$ correspond to the air flow rates when the fan is operating at medium and high speeds.

3.3.1 Reachability analysis

We are interested in performing reachability analysis of the hybrid model, which we run using SpaceEx ([7]). Notice that in this case we do not discretise time and consider a continuous time horizon of 2 hours. We consider two different initial conditions: in the first experiment we select an initial condition equal to $T_{z_1} = 15^oC$ and $T_{sa} = 15^oC$, while in the second we set $T_{z_1} = 20^oC$ and $T_{sa} = 20^oC$. The resulting reach tube for the both experiments is shown in Figure 8a.



(a) Initial condition: $T_{z_1} = 15^oC$, $T_{sa} = 15^oC$

(b) Initial condition: $T_{z_1} = 20^oC$, $T_{sa} = 20^oC$

Figure 8: Third case study: reach tubes obtained from two different initial conditions

In Figure 8a we can see that the model initially is in state $(O, -)$ and jumps to a new state (H, Op) such that warm outside air is pumped into the zone (due to the low temperature of the initial conditions). From (H, Op) it switches to (M, Op) (notice the reduction in the gradient between the variables $T_{sa} \in [15\ 18]$, $T_{z_1} \in [17\ 19]$) and eventually switches back to $(O, -)$ in order to maintain the temperature within the comfort region. For Figure 8b, the reach tube shows that the system remains within the initial state $(O, -)$ over the whole time horizon.

4 Conclusions

This paper has presented a library of CPS models for BAS. The BAS modelling framework comprises three different types of complexities (stochasticity, number of continuous variables,

number of discrete modes) and is modular such that various BAS components can be composed. We illustrate the use of this BAS components library via three case studies, each of which highlights a different side of the complexity trade off and solves a different problem (simulation, (probabilistic) reachability analysis, and strategy synthesis respectively). Current work is developed towards obtaining a compositional tool that is able to allow for easy construction of BAS models and for interfacing with different (i) verification tools for performing analysis and (ii) synthesis tools for computation of optimal strategies.

Acknowledgements

This work has been funded by the European Commission in the Seventh Framework Programme project AMBI under Grant No.: 324432 and is in part supported by the Alan Turing Institute, UK and Malta's ENDEAVOUR Scholarships Scheme. The authors would also like to thank Dario Cattaruzza, Sofie Haesaert and Honeywell Laboratories, Prague for their fruitful feedback.

References

[1] Hamza Belkhouane, Jan Hensen, and Shady Attia. Thermal comfort models for net zero energy buildings in hot climates. In *Second International Conference on Energy and Indoor Environment for Hot Climates*. Doha, 2017.

[2] Dario Cattaruzza, Alessandro Abate, Peter Schrammel, and Daniel Kroening. Unbounded-time analysis of guarded LTI systems with inputs by abstract acceleration. In *International On Static Analysis*, pages 312–331. Springer, 2015.

[3] Nathalie Cauchi, Khaza Anuarul Hoque, Alessandro Abate, and Mariëlle Stoelinga. Efficient probabilistic model checking of smart building maintenance using fault maintenance trees. *arXiv preprint arXiv:1801.04263*, 2018.

[4] Scott Cotton, Goran Frehse, and Olivier Lebeltel. The spaceex modeling language, 2010.

[5] Drury B Crawley, Jon W Hand, Michaël Kummert, and Brent T Griffith. Contrasting the capabilities of building energy performance simulation programs. *Building and environment*, 43(4):661–673, 2008.

[6] Iulia Dragomir, Viorel Preoteasa, and Stavros Tripakis. The refinement calculus of reactive systems toolset. *arXiv preprint arXiv:1710.08195*, 2017.

[7] Goran Frehse, Colas Le Guernic, Alexandre Donzé, Scott Cotton, Rajarshi Ray, Olivier Lebeltel, Rodolfo Ripado, Antoine Girard, Thao Dang, and Oded Maler. SpaceEx: Scalable verification of hybrid systems. In *Computer Aided Verification*, pages 379–395. Springer, 2011.

[8] Sofie Haesaert, Nathalie Cauchi, and Alessandro Abate. Certified policy synthesis for general markov decision processes: An application in building automation systems. *Performance Evaluation*, 117:75–103, 2017.

[9] Sofie Haesaert, Sadegh Esmaeil Zadeh Soudjani, and Alessandro Abate. Verification of general Markov decision processes by approximate similarity relations and policy refinement. *SIAM Journal on Control and Optimization*, 55(4):2333–2367, 2017.

[10] Ernst Moritz Hahn, Arnd Hartmanns, Holger Hermanns, and Joost-Pieter Katoen. A compositional modelling and analysis framework for stochastic hybrid systems. *Formal Methods in System Design*, 43(2):191–232, 2013.

[11] Ondrej Holub, Majid Zamani, and Alessandro Abate. Efficient hvac controls: A symbolic approach. In *Control Conference (ECC), 2016 European*, pages 1159–1164. IEEE, 2016.

[12] Woohyun Kim and Srinivas Katipamula. A review of fault detection and diagnostics methods for building systems. *Science and Technology for the Built Environment*, pages 1–18, 2017.

[13] Niels Rode Kristensen, Henrik Madsen, and Sten Bay Jørgensen. Parameter estimation in stochastic grey-box models. *Automatica*, 40(2):225–237, February 2004.

[14] Y. Ma, A. Kelman, A. Daly, and F. Borrelli. Predictive control for energy efficient buildings with thermal storage: modeling, stimulation, and experiments. *Control Systems, IEEE*, 32(1):44–64, February 2012.

[15] S. Privara, J. Cigler, Z. Vana, F. Oldewurtel, C. Sagerschnig, and E. Zacekova. Building modeling as a crucial part for building predictive control. *Energy and Buildings*, 56:8–22, 2013.

[16] S. Esmaeil Zadeh Soudjani and A. Abate. Aggregation and Control of Populations of Thermostatically Controlled Loads by Formal Abstractions. *Control Systems Technology, IEEE Transactions on*, 23(3):975–990, May 2015.

[17] Sadegh Esmaeil Zadeh Soudjani, Caspar Gevaerts, and Alessandro Abate. Faust 2: Formal Abstractions of Uncountable-STate STochastic processes. In *TACAS*, volume 15, pages 272–286, 2015.

[18] Wei Yu, Baizhan Li, Hongyuan Jia, Ming Zhang, and Di Wang. Application of multi-objective genetic algorithm to optimize energy efficiency and thermal comfort in building design. *Energy and Buildings*, 88:135–143, 2015.

[19] Rongpeng Zhang and Tianzhen Hong. Modeling of {HVAC} operational faults in building performance simulation. *Applied Energy*, 202:178 – 188, 2017.

Appendix

Discrete-time models for heating system of two zones with deterministic or stochastic dynamics

We present the corresponding system matrices of the three models $\mathbf{M}_d, \mathbf{M}_{da}, \mathbf{M}_s$ described in Sec. 3.1. $\mathbf{M}_d$ is given by (1) and is characterised by the following system matrices:

$$A = \begin{bmatrix} 0.6682 & 0 & 0.02632 & 0 \\ 0 & 0.6830 & 0 & 0.02096 \\ 1.0005 & 0 & -0.000499 & 0 \\ 0 & 0.8004 & 0 & 0.1996 \end{bmatrix},\ B = \begin{bmatrix} 0.1320 \\ 0.1402 \\ 0 \\ 0 \end{bmatrix},\ Q_d = \begin{bmatrix} 3.4364 \\ 2.9272 \\ 13.0207 \\ 10.4166 \end{bmatrix}.$$

$\mathbf{M}_{da}$ is given by (2) and is characterised by the same system matrices used for $\mathbf{M}_d$ together with,

$$F_{da} = \begin{bmatrix} 8.760e{-}06 & 0 \\ 0 & 2.704e{-}07 \\ 0 & 0 \\ 0 & 0 \end{bmatrix},\ Q_{da} = \begin{bmatrix} 3.3378 \\ 2.9106 \\ 13.0207 \\ 10.4166 \end{bmatrix}.$$

$\mathbf{M}_s$ is given by (3) and is characterised by the same system matrices used for $\mathbf{M}_d$ together with,

$$\Sigma = \begin{bmatrix} 0.0774 & 0 & 0 & 0 \\ 0 & 0.0774 & 0 & 0 \\ 0 & 0 & 0.3872 & 0 \\ 0 & 0 & 0 & 0.3098 \end{bmatrix}.$$

In all cases we use,

$$T_{w_{ss}} = 18^oC,\ T_{SP} = 20^oC,\ T_{sw,b_{ss}} = 75^oC,\ T_{z_{1_{ss}}} = 20^oC,$$
$$T_{z_{2_{ss}}} = 20^oC,\ T_{rw,r_{1_{ss}}} = 35^oC,\ T_{rw,r_{2_{ss}}} = 35^oC.$$

We perform a simulation run of all three models over a two-day period, with

$$u[k] = \begin{cases} 20^oC & \text{k is between 8am - 12pm, 1pm - 6pm,} \\ 18^oC & \text{otherwise,} \end{cases}$$

and depict the resulting simulation runs for the temperature within zone 1 in Figure 3.

Reachability analysis using Axelarator

To perform reachability analysis using Axelarator we need to use the following commands in command line,

```
../aa/axelerator Dynamics.txt -init
"[]" -sguard "[]" -inc -mpi -u
```

where the file `Dynamics.txt` contains the corresponding system matrices and defines the dimensions of both the state space and control inputs of the underlying model. The initial conditions are defined using `-init "[]"` and `-sguard "[]"` will force the tool to stay inside the safe region (if possible) defined within `"[]"`. The commands `-inc -mpi -u` set the conditions of the problem such that Axelarator makes use of incremental search with multiple precision intervals and to process unsound results. We also provide Axelerator with the safe set defined in the form of a polyhedral,

$$\begin{bmatrix} T_{z_1} \\ T_{z_2} \end{bmatrix} > \begin{bmatrix} 19.5 \\ 19.5 \end{bmatrix} \wedge \begin{bmatrix} T_{z_1} \\ T_{z_2} \end{bmatrix} < \begin{bmatrix} 20.5 \\ 20.5 \end{bmatrix}.$$

This safe set is used as a reference once the resulting reach tube is computed. The results obtained using Axelarator are in the form of polyhedral sets which define the reach tube of

the underlying system over the N time steps. For $\mathbf{M}_d$ the polyhedral sets are given as,

$$\begin{bmatrix}
T_{z_1} & < & 22.2282, & T_{z_2} & < & 22, \\
T_{rw,r_1} & < & 40, & T_{rw,r_2} & < & 40, \\
-T_{z_1} & < & -10.0899, & -T_{z_2} & < & -5.40334, \\
-T_{rw,r_1} & < & 105.958, & -T_{rw,r_2} & < & -11.1481, \\
T_{z_1}+T_{z_2} & < & 44, & T_{z_1}+T_{rw,r_1} & < & 62, \\
T_{z_1}+T_{rw,r_2} & < & 62, & T_{z_1}-T_{z_2} & < & 9.40198, \\
T_{z_1}-T_{rw,r_1} & < & 116.097, & T_{z_1}-T_{rw,r_2} & < & 1.12788, \\
-T_{z_1}+T_{z_2} & < & 7, & -T_{z_1}+T_{rw,r_1} & < & 25, \\
-T_{z_1}+T_{rw,r_2} & < & 25, & -T_{z_1}-T_{z_2} & < & -15.4932, \\
-T_{z_1}-T_{rw,r_1} & < & 95.8203, & -T_{z_1}-T_{rw,r_2} & < & -21.238, \\
T_{z_2}+T_{rw,r_1} & < & 62, & T_{z_2}+T_{rw,r_2} & < & 62, \\
T_{z_2}-T_{rw,r_1} & < & 114.105, & T_{z_2}-T_{rw,r_2} & < & -5.50237, \\
-T_{z_2}+T_{rw,r_1} & < & 25, & -T_{z_2}+T_{rw,r_2} & < & 25, \\
-T_{z_2}-T_{rw,r_1} & < & 100.555, & -T_{z_2}-T_{rw,r_2} & < & -16.5515, \\
T_{rw,r_1}+T_{rw,r_2} & < & 80, & T_{rw,r_1}-T_{rw,r_2} & < & 10, \\
-T_{rw,r_1}+T_{rw,r_2} & < & 126.441, & -T_{rw,r_1}-T_{rw,r_2} & < & 94.8101
\end{bmatrix},$$

whereas for $\mathbf{M}_{da}$

$$\begin{bmatrix}
T_{z_1} & < & 22.3242, & T_{z_2} & < & 22, \\
T_{rw,r_1} & < & 40, & T_{rw,r_2} & < & 40, \\
-T_{z_1} & < & -10.1225, & -T_{z_2} & < & -5.38875, \\
-T_{rw,r_1} & < & 109.275, & -T_{rw,r_2} & < & -11.1512, \\
T_{z_1}+T_{z_2} & < & 44, & T_{z_1}+T_{rw,r_1} & < & 62, \\
T_{z_1}+T_{rw,r_2} & < & 62, & T_{z_1}-T_{z_2} & < & 9.50273, \\
T_{z_1}-T_{rw,r_1} & < & 119.446, & T_{z_1}-T_{rw,r_2} & < & 1.20718, \\
-T_{z_1}+T_{z_2} & < & 7, & -T_{z_1}+T_{rw,r_1} & < & 25, \\
-T_{z_1}+T_{rw,r_2} & < & 25, & -T_{z_1}-T_{z_2} & < & -15.5113, \\
-T_{z_1}-T_{rw,r_1} & < & 99.1041, & -T_{z_1}-T_{rw,r_2} & < & -21.2737, \\
T_{z_2}+T_{rw,r_1} & < & 62, & T_{z_2}+T_{rw,r_2} & < & 62, \\
T_{z_2}-T_{rw,r_1} & < & 117.336, & T_{z_2}-T_{rw,r_2} & < & -5.51993, \\
-T_{z_2}+T_{rw,r_1} & < & 25, & -T_{z_2}+T_{rw,r_2} & < & 25, \\
-T_{z_2}-T_{rw,r_1} & < & 103.886, & -T_{z_2}-T_{rw,r_2} & < & -16.5399, \\
T_{rw,r_1}+T_{rw,r_2} & < & 80, & T_{rw,r_1}-T_{rw,r_2} & < & 10, \\
-T_{rw,r_1}+T_{rw,r_2} & < & 129.684, & -T_{rw,r_1}-T_{rw,r_2} & < & 98.1239.
\end{bmatrix}$$

Probabilistic reachability analysis using FAUST^2

To solve this problem and achieve low errors within a computationally feasible time frame we abstract the model $\mathbf{M}_s$ such that

$$x^T = [T_{z_1}\ T_{z_2}]^T$$

(the states of interest and we fix the rest of the state to steady-state). Based on this model, we construct a stochastic kernel in the form of a Gaussian conditional distribution, $\mathcal{N}(f(x,u),\Sigma)$ where

$$f(x,u) = Ax + Bu + Q_d$$

(cf. (3)) and

$$\Sigma = diag(\Delta[\sigma_{z_1}^2, \sigma_{z_2}^2])$$

. The input space of the process is set to [15 22], while the safe-set is defined as

$$\begin{bmatrix} 19.5 & 19.5 \\ 20.5 & 20.5 \end{bmatrix}.$$

We select the `PCTL Safety` option in FAUST^2 to compute the analysis. The model is abstracted based on adaptive partitioning, with a partitioning error of $\epsilon = 10^{-5}$, to obtain the discretised transition kernel. The maximal safety probability for each partition is computed, based on the transition kernel, recursively over the whole time horizon $N = 6$.

Discrete-time models for two-zone heating setup with large number of continuous variables

We present the corresponding system matrices of the model $\mathbf{M}_c$ described in Subsection 3.2 as:

$$A_c = \begin{bmatrix} 0.9998 & 6.54e{-9} & 2.23e{-5} & 2.23e{-5} & 2.23e{-5} & 4.88e{-14} & 4.88e{-14} \\ 5.739e{-9} & 0.9998 & 4.27e{-14} & 4.27e{-14} & 2.23e{-5} & 2.23e{-5} & 2.23e{-5} \\ 0.0005 & 1.27e{-12} & 0.9989 & 6.54e{-9} & 6.54e{-9} & 7.13e{-18} & 7.13e{-18} \\ 0.0005 & 1.27e{-12} & 6.54e{-9} & 0.9989 & 6.54e{-9} & 7.13e{-18} & 7.13e{-18} \\ 0.00051 & 0.00058 & 5.73e{-9} & 5.73e{-9} & 0.9989 & 6.54e{-9} & 6.54e{-9} \\ 1.11e{-12} & 0.00058 & 6.25e{-18} & 6.25e{-18} & 6.54e{-9} & 0.9989 & 6.54e{-9} \\ 1.11e{-12} & 0.00058 & 6.25e{-18} & 6.25e{-18} & 6.54e{-9} & 6.54e{-9} & 0.9980 \end{bmatrix}, \quad B_c = \begin{bmatrix} 0.000122 \\ 0.000122 \\ 3.58e{-8} \\ 3.58e{-8} \\ 6.72e{-8} \\ 3.58e{-8} \\ 3.58e{-8} \end{bmatrix},$$

$$F_c = \begin{bmatrix} 1.027e{-8} & 5.734e{-9} & 7.31e{-9} & 2.71e{-15} & 0.0013 & 0.0014 \\ 1.91e{-7} & 5.73e{-9} & 1.39e{-17} & 1.24e{-6} & 0.0021 & 0.0022 \\ 2.00e{-12} & 0.0005 & 2.13e{-12} & 3.96e{-19} & 3.84e{-7} & 3.84e{-7} \\ 0.0009 & 1.11e{-12} & 2.13e{-12} & 3.96e{-19} & 3.84e{-7} & 3.84e{-7} \\ 3.90e{-11} & 2.09e{-12} & 1.87e{-12} & 3.63e{-10} & 9.78e{-7} & 9.78e{-7} \\ 3.72e{-11} & 0.00051 & 2.042e{-21} & 3.63e{-10} & 6.41e{-7} & 6.41e{-7} \\ 0.01708 & 1.11e{-12} & 2.04e{-21} & 3.63e{-10} & 6.40e{-7} & 6.41e{-7} \end{bmatrix}, \quad Q_c = \begin{bmatrix} 0.2482 \\ -0.0055 \\ 0.1270 \\ 0.0201 \\ 0.0145 \\ 0.0144 \\ 0.0145 \end{bmatrix}.$$

We model the disturbances as random external effects affecting the room temperature dynamics as $T_{out}[k] \sim \mathcal{N}(9,1),\ T_{hall}[k] \sim \mathcal{N}(15,1),\ CO_{2_i}[k] \sim \mathcal{N}(500,100), i \in \{1,2\},\ T_{rw,r_i}[k] \sim \mathcal{N}(35,5), i \in \{1,2\}$.

Next, we present the abstract models $\mathbf{M}_{c_a}, a = \{4,\ldots,1\}$ taking the same form as (4) with

Model	$\mathbf{x}_c^T$	$\mathbf{d}_c^T$
$\mathbf{M_{c_4}}$	$[T_{z_1}\ T_{w_5}\ T_{w_2}\ T_{w_7}]^T$	$[T_{out}\ T_{hall}\ CO_{2_1}\ T_{rw,r_1}\ T_{z_2}]^T$
$\mathbf{M_{c_3}}$	$[T_{z_1}\ T_{w_5}\ T_{w_2}]^T$	$[T_{out}\ T_{hall}\ CO_{2_1}\ T_{rw,r_1}]^T$
$\mathbf{M_{c_2}}$	$[T_{z_1}\ T_{w_2}]^T$	$[T_{out}\ CO_{2_1}\ T_{rw,r_1}]^T$
$\mathbf{M_{c_1}}$	$[T_{z_1}]^T$	$[T_{out}\ CO_{2_1}\ T_{rw,r_1}]^T$

and, T_{z_2} is $\sim \mathcal{N}(20,1)$. For $\mathbf{M_{c_4}}$ we have

$$A_{c_4} = \begin{bmatrix} 0.9998 & 2.23e{-5} & 2.23e{-5} & 2.23e{-5} \\ 0.00058 & 0.9989 & 6.54e{-9} & 6.54e{-9} \\ 0.00058 & 6.54e{-9} & 0.9989 & 6.54e{-9} \\ 0.00051 & 5.73e{-9} & 5.73e{-9} & 0.9989 \end{bmatrix},\ B_{c_4} = \begin{bmatrix} 0.00012 \\ 3.5859e{-8} \\ 3.5859e{-8} \\ 3.1424e{-8} \end{bmatrix},$$

$$F_{c_4} = \begin{bmatrix} 1.02e{-8} & 5.73e{-9} & 7.31e{-9} & 0.0013 & 6.54e{-9} \\ 2.00e{-12} & 0.0005 & 2.13e{-12} & 3.84e{-7} & 1.27e{-12} \\ 0.0009 & 1.11e{-12} & 2.13e{-12} & 3.84e{-7} & 1.27e{-12} \\ 1.75e{-12} & 9.79e{-13} & 1.87e{-12} & 3.37e{-7} & 0.00058 \end{bmatrix},\ Q_{c_4} = \begin{bmatrix} 0.2482 \\ 0.1270 \\ 0.0145 \\ 0.0145 \end{bmatrix},$$

while for $\mathbf{M}_{c_3}$,

$$A_{c_3} = \begin{bmatrix} 0.9998 & 2.23e{-5} & 2.23e{-5} \\ 0.00058 & 0.9989 & 6.54e{-9} \\ 0.00058 & 6.54e{-9} & 0.9980 \end{bmatrix},\ B_{c_3} = \begin{bmatrix} 0.000122 \\ 0.000122 \\ 3.58e{-8} \end{bmatrix},$$

$$F_{c_3} = \begin{bmatrix} 6.29e{-9} & 5.73e{-9} & 7.31e{-9} & 0.0013 \\ 1.22e{-12} & 0.00051 & 2.13e{-12} & 3.84e{-7} \\ 0.00056 & 1.11e{-12} & 2.13e{-12} & 3.84e{-7} \end{bmatrix},\ Q_{c_3} = \begin{bmatrix} 0.2482 \\ 0.1270 \\ 0.0145 \end{bmatrix}.$$

For $\mathbf{M}_{c_2}$ the system matrices are

$$A_{c_2} = \begin{bmatrix} 0.9998 & 2.237e{-5} \\ 0.00058 & 0.9989 \end{bmatrix},\ B_{c_2} = \begin{bmatrix} 0.00012 \\ 3.58e{-8} \end{bmatrix},$$

$$F_{c_2} = \begin{bmatrix} 1.027e{-8} & 7.31e{-9} & 0.0013 \\ 0.00091 & 2.13e{-12} & 3.84e{-7} \end{bmatrix},\ Q_{c_2} = \begin{bmatrix} 0.2482 \\ 0.1270 \end{bmatrix}.$$

and $\mathbf{M}_{c_1}$ is described using

$$A_{c_1} = [\,0.9998\,], B_{c_1} = [\,0.000122\,], \qquad F_{c_1} = [\,6.31e{-5}\ 7.31e{-9}\ 0.0013\,],\ Q_{c_1} = [\,0.2482\,].$$

Models for heating system setup with multiple switching controls

To construct the hybrid model we use $T_{w_{ss}} = 18^oC,\ T_{out} = 25^oC,\ T_{SP} = 20^oC,$ $\delta = 1^oC,\ \delta_2 = 2^oC,\ \delta_3 = 3^oC,\ \delta_4 = 4^oC,\ \delta_5 = 5^oC,\ m_{a,med} = 10m^3/hr, m_{a,high} = 15m^3/hr\ CO_{2_{ss}} = 500ppm$. The continuous dynamics are composed via the following simplifying assumptions: (i) the outside air temperature is fixed $T_{out} = 25^oC$ and is used to warm up the zone such the temperature set-point $T_{SP} = 20^oC$ is maintained; (ii) we fix $CO_{2_{1_{ss}}}$; (iii) there is a constant wall temperature $T_{w_{ss}}$; (iv) there are no radiators within the zone; and (v) there is no process noise. The resulting continuous state models for each discrete mode using the corresponding models presented in Table **??**.

Discrete state	**Continuous space dynamics**
$q = (O, -)$	$\dot{T}_{z_1} = -0.0116T_{z_1}(t) + 0.2565$ $\dot{T}_{sa} = 0.0183T_{z_1}(t) - 0.0183T_{sa}(t)$
$q = (M, Op)$	$\dot{T}_{z_1} = -0.0292T_{z_1}(t) + 0.0176T_{sa}(t) + 0.2565$ $\dot{T}_{sa} = 0.0183T_{z_1}(t) - 0.0185T_{sa}(t) + 0.005$
$q = (M, Cl)$	$\dot{T}_{z_1} = -0.0292T_{z_1}(t) + 0.0176T_{sa}(t) + 0.2565$ $\dot{T}_{sa} = 0.0183T_{z_1}(t) - 0.0183T_{sa}(t)$
$q = (H, Op)$	$\dot{T}_{z_1} = -0.038T_{z_1}(t) + 0.0264Tsa(t) + 0.2565$ $\dot{T}_{sa} = 0.0183T_{z_1}(t) - 0.0186T_{sa}(t) + 0.0076$
$q = (H, Cl)$	$\dot{T}_{z_1} = -0.038T_{z_1}(t) + 0.0264Tsa(t) + 0.2565$ $\dot{T}_{sa} = 0.0186T_{z_1}(t) - 0.0186T_{sa}(t).$

Reachability analysis using SpaceEx

We first implement the hybrid system delineated using Figure 7 within SpaceEx using SX (the SpaceEx modelling language [4]). We further bound the zone temperature to lie between $T_{z_1} \in [10\ 30]$, while supply temperature to lie between $T_{sa} \in [15\ 30]$: corresponding to physically feasible states when BAS is operating in a good condition. This model file is loaded into SpaceEx and the input model is converted into a flat hybrid automaton representation over which reachability analysis can be performed. Next, we set-up the configuration file defining (i) the initial states in the form of `"Tz1==15&Tsa==20&loc()==off"`, where `"off"` refers to the initial state label, (ii) any forbidden states (in our case study there is none), (iii) the time-horizon, and (iv) the direction of the reach sets (we select `oct`, but similar results are achieved when the direction of reach set was set to `box`). Once the configuration file is loaded, the reachability analysis algorithm is run over the defined time horizon, which in our case corresponds to two hours and the reachable sets are generated (cf. Figure 8).