SMT-Based Analysis of Virtually Synchronous Distributed Hybrid Systems*

Kyungmin Bae
SRI International

Peter Csaba Ölveczky
University of Oslo

Sooho Kong
Carnegie Mellon University

Sicun Gao
MIT CSAIL

Edmund M. Clarke
Carnegie Mellon University

ABSTRACT

This paper presents general techniques for verifying virtually synchronous distributed control systems with interconnected physical environments. Such cyber-physical systems (CPSs) are notoriously hard to verify, due to their combination of nontrivial continuous dynamics, network delays, imprecise local clocks, asynchronous communication, etc. To simplify their analysis, we first extend the PALS methodology—that allows to abstract from the timing of events, asynchronous communication, network delays, and imprecise clocks, as long as the infrastructure guarantees bounds on the network delays and clock skews—from real-time to hybrid systems. We prove a bisimulation equivalence between Hybrid PALS synchronous and asynchronous models. We then show how various verification problems for synchronous Hybrid PALS models can be reduced to SMT solving over nonlinear theories of the real numbers. We illustrate the Hybrid PALS modeling and verification methodology on a number of CPSs, including a control system for turning an airplane.

Keywords
Distributed hybrid systems; SMT; synchronizers; PALS

1. INTRODUCTION

Virtually synchronous distributed hybrid systems consist of a number of distributed controllers—where each controller may interact with its physical environment having continuous dynamics which, furthermore, can be correlated—that should logically behave in a synchronous way. This class of cyber-physical systems (CPSs) includes avionics, robotics, automotive, and medical systems. Designing and analyzing such systems is difficult because of the interrelated continuous behaviors combined with clock skews, network delays, execution times, and so on.

*A key step towards achieving manageable modeling and verification techniques for this complex class of CPSs is to extend the PALS framework to distributed hybrid systems. The PALS (physically asynchronous, logically synchronous) methodology [1, 3, 15] was developed to reduce the design and analysis of a virtually synchronous distributed real-time system (i.e., one without continuous behaviors) to the much simpler tasks of designing and analyzing the underlying synchronous models, provided that the network infrastructure can guarantee bounds on computation times, network delays, and imprecision of the local clocks. In this paper we introduce Hybrid PALS for virtually synchronous distributed hybrid systems. Hybrid PALS extends the approach in [5] to achieve a bisimulation equivalence between Hybrid PALS synchronous models and their asynchronous counterparts. This means that verifying a virtually synchronous distributed hybrid system reduces to verifying its underlying synchronous model. Hybrid PALS allows us to abstract from asynchronous communication, network delays, message buffering, etc. However, the times at which physical states are sampled or actuator commands are sent to the environment cannot be abstracted away. Since these events are triggered by imprecise local clocks, we must also take into account those clocks. Furthermore, the physical environments of different components are often tightly coupled, so that the continuous dynamics of the entire system becomes nonlinear. For these reasons, analysis techniques for event-based systems (such as hybrid automata) or linear systems cannot be easily used to analyze Hybrid PALS models.

This paper presents SMT solving techniques to address the challenges of analyzing Hybrid PALS models. The verification of a synchronous Hybrid PALS model, which involves (nonlinear) ordinary differential equations (ODEs) and clock skews, is reduced to checking the satisfiability of SMT formulas over the real numbers, which is decidable up to any user-given precision [8, 10]. We show how standard verification problems for hybrid systems, such as bounded reachability, unbounded time inductive reasoning, and compositional assume-guarantee reasoning, can be encoded as SMT formulas for synchronous Hybrid PALS models.

We have applied our techniques on a range of non-trivial nonlinear systems, including: a control system for turning an airplane, a networked controller for physically connected water tanks, and a networked thermostat controller for interconnected adjacent rooms. These case studies involve nonlinear ODEs and continuous connections between different components, and take into account network delays, clock skews, asynchronous communication, execution times, etc.
To summarize, the new contributions in this paper (also compared to [5]) are: (i) more refined and complete Hybrid PALS models; (ii) a bisimulation result between synchronous and asynchronous Hybrid PALS models; (iii) general SMT techniques for analyzing synchronous Hybrid PALS models (as opposed to showing only concrete analysis of toy examples in [5]); and (iv) illustrating the effectiveness of Hybrid PALS and the proposed verification methodology on complex examples and hybrid systems benchmarks.

The rest of the paper is organized as follows. Section 2 discusses related work. Section 3 gives a background on PALS. Section 4 introduces Hybrid PALS. Section 5 shows SMT encodings for Hybrid PALS models and their analysis. Section 6 gives an overview of the Hybrid PALS case studies. Finally, Section 7 gives some concluding remarks.

2. RELATED WORK

PALS [1, 3, 15] targets distributed real-time systems, whose absence of continuous behaviors means that the timing of events, and hence local clocks, can be abstracted away in the synchronous models, which can therefore be verified by standard model checking techniques. In contrast, (synchronous) Hybrid PALS models must take both continuous behaviors and clock skew into account and therefore cannot be analyzed using such techniques for discrete systems.

The initial steps towards a hybrid extension of PALS were taken in [5]. However, the formal models of Hybrid PALS in [5] are very different from the models in this work, so that a bisimulation equivalence could not be provided in [5]. In this paper, Hybrid PALS models are significantly redefined to obtain a bisimulation between synchronous and distributed hybrid models, and to allow more general sampling and response times of sensors and actuators. For example, components in the same synchronous state may have different local times in [5], but those times are synchronized in this paper to properly model the continuous behavior for tightly coupled environments. Furthermore, [5] shows that two interconnected thermostats can be verified using dReal, but does not present general SMT techniques for analyzing synchronous Hybrid PALS models.

Our case studies on networks of identical hybrid systems are related to symmetry-reduction approaches for networks of timed or hybrid automata (e.g., [6, 11, 13]), and their compositional analysis for any number of identical processes is related to [12]. Such work uses hybrid or timed automata where communication is specified using joint synchronous actions, whereas our work focuses on time-triggered systems with nonlinear dynamics where communication is governed by real-time constraints, taking into account network delays, execution times, and clock skews, and where the local environments of tightly coupled components continuously interact with each other. In addition, Hybrid PALS considers general virtually synchronous distributed hybrid systems (e.g., the airplane example in our paper), besides symmetric distributed hybrid systems.

3. PRELIMINARIES ON PALS

PALS transforms a multirate synchronous design SD into a distributed real-time system MA(SD, T) that satisfies the same temporal logic properties, provided that the underlying infrastructure assures bounds $F = (ε, o_{min}, o_{max}, p_{min}, p_{max})$ with: (i) $ε ≥ 0$ the maximal skew of any local clock with respect to the global clock, (ii) $[p_{min}, p_{max}]$ time bounds for executing a transition, and (iii) $[o_{min}, o_{max}]$ time bounds for the network transmission delay. This section overviews the synchronous models SD, the distributed models MA(SD, T), and their relationship (we refer to [3, 15] for details).

3.1 Discrete Synchronous Models

The synchronous model SD is specified as an ensemble of (nondeterministic) state machines with input and output ports. In each iteration, a machine performs a transition based on its current state and its inputs, proceeds to the next state, and generates new outputs for the next iteration.

Definition 1. A typed machine $M = (D_i, S, D_o, δ_M)$ is composed of: (i) $D_i = D_{i1} × · · · × D_{in}$ an input set (a value to the k-th input port is an element of $D_{ik}$), (ii) $S$ a set of states, (iii) $D_o = D_{o1} × · · · × D_{on}$ an output set, and (iv) $δ_M ⊆ (D_i × S) × (S × D_o)$ a total transition relation.

A collection $\{M_j\}_{j∈J_F}$ of state machines with different rates can be composed into a multirate ensemble $E_T$ with global period $T$, as illustrated in Fig. 1, where the period of a slow typed machine $s ∈ J_S$ (with rate(s) = $k$) is $k$ times the period of a fast machine $f ∈ J_F$ with rate(f) = $k > 1$. A wiring diagram connects the input and output ports, so that there are no connections between two fast machines. In each round of $E_T$, all components perform a transition in lockstep. A fast machine $f$ is slowed down and performs $k = rate(f)$ internal transitions in one global synchronous step. Since a fast machine produces $k$-tuples of outputs in one step, input adaptors are used to generate single values (e.g., the last value, or the average of the $k$ values) for a slow machine. Likewise, a single output from a slow machine is adapted to a $k$-tuple of inputs for a fast machine.

This synchronous composition of an ensemble $E_T$ is thus equivalent to one machine $M_{E_T} = (D_{E_T}, S_{E_T}, D_{E_o}, δ_{M_{E_T}})$. If a machine in $E_T$ has a feedback wire connected to itself or to another component, then the output becomes an input of the destination in the next iteration. That is, $M_{E_T}$’s states $S_{E_T}$ consist of the states of its subcomponents $M_j$ and the “feedback” outputs. For example, $M_{E_j}$ of the ensemble $E_T$ in Fig. 1 is the machine given by the outer box.

Definition 2. The transition system for $M_{E_T}$ is a tuple $ts(M_{E_T}) = (S_{E_T} × D_{E_o}, →_{E_T})$, where ($i_1, s_1, i_2, s_2, o$) if an iff an event in state $s_1$ with input $i_1$ from the interface has a transition to state $s_2$ (i.e., $s_2, o$) $∈ δ_{M_{E_j}}$.

3.2 PALS Distributed Real-Time Models

Each component in the distributed model MA($E_T$, T) is composed of a machine in $E_T$ and wrappers around it, as depicted in Fig. 2. In MA($E_T$, T), each machine performs transitions at its own rate according to its local clock. At the beginning of its period, it reads input from the layer above, performs a transition, and then generates output. A wrapper has I/O buffers, timers, and access to the local clock of the machine. A PALS wrapper has the same period.
times we cannot abstract from the time when a continuous value
of the fast machine to its outer layer at a global period T.

Notice that a fast machine $M_f$ may not be able to finish all
of its $k$ transitions in a global round, but only $k'$ transitions
before the outputs must be sent. If $k < k'$, then the $k$-
machine wrapper only sends the first $k$ values. The input
adapter of each input port whose source is
and sets its backoff timer to $2k - \mu_{\text{min}}$. When the execution
of the inner components ends and the backoff timer expires,
the contents of the output buffer are sent out.

An input adapter wrapper receives the inputs from the
PALS wrapper and applies input adaptors for each period $T$.
A $k$-machine wrapper extracts each value from the $k$-tuple
input and delivers it to the enclosed fast machine at each
fast period $T/k$, and delivers the $k$-tuples from the outputs
of the fast machine to its outer layer at a global period $T$.

Figure 2: The wrapper hierarchies in $\mathcal{MA}(E_T, \Gamma)$.

4. HYBRID PALS

This section introduces Hybrid PALS, which extends PALS
to distributed hybrid systems. In PALS, the time when an
event takes place does not matter, as long as it happens
within a certain time interval. However, in hybrid systems,
we cannot abstract from the time when a continuous value
is read or an actuator command is given (both of which depend
on a component’s local clock), and thus those times
are also included in the synchronous Hybrid PALS models.

4.1 Controlled Physical Environments

A state of a physical environment of machine $M$ is given
by a tuple $\vec{v} = (v_1, \ldots, v_k) \in \mathbb{R}^k$ of its physical parameters
$x = (x_1, \ldots, x_k)$. The behavior of $\vec{x}$ can be modeled by
ODEs that specify trajectories $\tau_1, \ldots, \tau_k$ of $\vec{x}$ over time.

A trajectory of duration $T$ is a function $\tau: [0, T] \rightarrow \mathbb{R}$.
The prefix of $\tau$ at time $u \in [0, T]$ is denoted by $\tau \preceq u$, and the suffix of $\tau$ at time $u$ is denoted by $\tau \succeq u$ that is,
$\tau(u) = \tau(t)$ for $t \in [0, u]$, and $\tau(u) = \tau(t) + u$ for
$u \in [0, T - t]$. Let $T$ denote the set of all trajectories.

A physical environment $E_M$ of machine $M$ is specified as a
controlled physical environment, defining any possible trajectory of its parameters $\vec{x}$ for the control commands from
$M$. For a state $\vec{v} \in \mathbb{R}^k$, a control command $a$, and a duration
$t \in \mathbb{R}$, a physical environment $E_M$ gives a trajectory $\vec{v}' \in T^t$
of its parameters $\vec{v}$ of duration $t$, as illustrated in Fig. 3.

Definition 4. A controlled physical environment is a tuple
$E_M = (C, \vec{v}, \Lambda)$, where: (i) $C$ is a set of control commands;
(ii) $\vec{x} = (x_1, \ldots, x_k)$ is a vector of real number variables; and
(iii) $\Lambda \subseteq (C \times \mathbb{R}^k) \times T^t$ is a physical transition relation
such that $(a, \vec{v}, t, \vec{v}') \in \Lambda$ iff for a control command $a \in C$
that lasts for duration $t$, $E_M$'s physical state $\vec{x}$ follows the trajectory $\vec{v}' \in T^t$ from state $\vec{v}(t) = \vec{v} \in \mathbb{R}^k$.

Many physical environments can be physically correlated,
and one local environment may immediately affect another
environment. Such correlations are naturally expressed as
time-invariant constraints $\forall t. \psi$ of physical parameters over
time $t$. For example, if parameter $x_1$ of $E_M$, $x_2$ must be equal
to parameter $x_2$ of $E_M$, then the time-invariant constraint is
the formula $\forall t. x_1(t) = x_2(t)$ with $t$ a variable over time.

Example 1. Consider a distributed CPS controller to roll
an airplane by moving its ailerons (flaps attached to the
end of the left or the right wing), illustrated in Fig. 4.
Each aileron subcontroller moves the corresponding aileron
towards the goal angle given by the main controller.
The subcontrollers and the main controller operate at different
rates. The objective of the main controller is to roll the
aircraft toward the goal angle specified by the pilot.

The physical environment $E_M$ of each subcontroller $M$
specifies the dynamics of the aileron angle $\varphi_M$ according to
the moving rate $r_M$ (the control command from $M$) by the

Figure 3: A controlled physical environment; e.g.,
$((a_1, v_1, t_2 - t_1, \tau_1), ((a_1', v_1, t_2 - t_1, \tau_1)) \in \Lambda$, etc.
ODE $\dot{x}_M = r_M$. The controlled physical environment is given by $E_M = (\mathbb{R}, x_M, \Lambda_M)$, with $\mathbb{R}$ the domain of $r_M$, and $\Lambda_M \subseteq (\mathbb{R} \times \mathbb{R} \times \mathbb{R}_{\geq 0}) \times T$ such that $((t_M, v_M, 15), \tau) \in \Lambda_M$ if and only if $\forall t \in [0, 15], \tau(t) = t_M + \int_0^t \dot{r}_M \, dt$.

The physical environment $E_{M\text{Main}}$ of the main controller specifies the dynamics of the roll angle $\phi$ using the ODEs $\dot{\phi} = \rho$ and $\dot{\rho} = \gamma(\phi - \rho)$, disregarding the yawing effect caused by the rolling, where $\phi$ is the rolling moment, and $\rho$ and $\gamma$ are their physical correlations. The controlled physical environment is $E_{M\text{Main}} = \{(\phi, \rho, \phi, \gamma, \Lambda_{M\text{Main}})\}$, with the singleton $\Lambda_{M\text{Main}}$, indicating that $E_{M\text{Main}}$ has no control command, and $\Lambda_{M\text{Main}} \subseteq \{(\phi, \rho, \phi, \gamma, \Lambda_{M\text{Main}})\}$ such that $((\phi(t), \rho(t), \phi(t), \gamma(t), \Lambda_{M\text{Main}})) \in \Lambda_{M\text{Main}}$ if and only if $\forall t \in [0, 60], [\tau_0, \tau_p]((t) = \int_0^\tau \dot{\tau}(t) \, dt) = \frac{t}{v_o}$.

The control angles $\xi_1$ and $\xi_2$ must always be the same as the respective aileron angles $x_1$ and $x_2$ of the subcontrollers. However, since the main controller and the subcontrollers have different periods with local clock skew, the ODEs of the subcontrollers cannot be plugged into $E_{M\text{Main}}$. Instead, their physical correlations are specified by the time-invariant constraint: $\forall t \in [0, 60], [\tau_0, \tau_p]((t) = \frac{x(t)}{v_o}) \cap [\tau_0, \tau_p]((t) = \frac{x(t)}{v_o})$.

### 4.2 Sampling and Response Timing

A controller $M$ interacts with its physical environment $E_M$ according to its local clock, which may differ from the global time by up to the maximal clock skew $\epsilon > 0$. Let $c_M : N \to R_{\geq 0}$ denote the global time $c_M(i)$ at the beginning of the $(i + 1)$-th period according to $M$'s local clock.

Figure 5 depicts the behavior of the controller $M$ with respect to $E_M$ in a PALS distributed model for an interval $[iT - \epsilon, (i + 1)T - \epsilon]$ for its period $T$. The $(i + 1)$-th period of $M$ begins at time $c_M(i) \in [iT - \epsilon, iT + \epsilon)$. Because of PALS bounds, $M$ has already received all the inputs at time $iT - \epsilon$. Next, the physical state $v_M(i)$ of $E_M$ is read at time $c_M(i) + t_M$ for some sampling time $t_M$. $M$ then executes its transition based on the inputs $i$, the sampled state $v_M(i)$, and the machine state $s$.

After the execution, the machine state changes to $s'$, and the new controller command $a$ is sent to $E_M$ at time $c_M(i) + \tau_R$ for some response time $t_R$ for the execution and the actuator processing. The new outputs $a$ are delivered to $M$'s observable part of the environment.

We assume that a control command $M$ to $E_M$ only depends on $M$'s current state $s$. In Figure 5, a current control command $a$ (by state $s$) remains effective until the execution of $M$ ends at time $u_M = c_M(i) + t_R$, and then a new control command $a'$ (by state $s'$) takes effect. That is, $E_M$ defines trajectories $\bar{\tau}$ of its physical parameters $\bar{\tau}$ in a time interval $[iT - \epsilon, (i + 1)T - \epsilon]$ of duration $T$ with respect to $(a, a', u_M)$.

**Definition 5.** Trajectories $\bar{\tau}$ of duration $T$ are realizable with respect to commands $a, a' \in C$ and a response duration $u \in \mathbb{R}$ for $E_M$, denoted by $\bar{\tau} \in R_{\mathbb{R}}^T E_M(a, a', u)$, if $((a, \bar{\tau}(0), u), \bar{\tau} \leq u) \in \Lambda$ and $((a', \bar{\tau}(u), T - u), \bar{\tau} \geq u) \in \Lambda$.

**Example 2.** Consider a subcontroller $M$ in Example 1 to move an aileron toward the specified angle. In each 15 ms round, beginning at time $c_M(i) \in (i \times 15 \text{ ms} - \epsilon, i \times 15 \text{ ms} + \epsilon)$, $M$ receives a goal angle $g_M$, sets a new moving rate $v_M$, based on $v_M$ and the observed angle $v_M$ and sends back $v_M$. $M$ is specified as the machine $(\mathbb{R}, \mathbb{R} \times \mathbb{R}, \delta_M, (\mathbb{R}, v_M))$, where $(g_M(i, t_M, v_M), ((i', t'_M, v'_M), o)) \in \delta_M$ holds if $i' = i + 1$, $t'_M = (g_M - t_M)/15$, and $o = v_M$. In practice, the sampling and response times depend on the machine instructions of a controller $M$ to perform these tasks, which are expressed as state transitions in our model. Therefore, we assume that the sampling times of $M$ depend on its state $s$, and the response times depend on its state $s$ and input $\bar{\tau}$. To compose $M$ with its physical environment $E_M$, we define the "interface" between them.

**Definition 6.** The interface of controller $M$ is defined by the projection functions $\bar{\tau} = (\pi_C, \pi_T, \pi_R, \pi_s)$, for state $s$ and input $\bar{\tau}: (i) \pi_C(s) = C$ the control command of $M$ to $E_M$; (ii) $\pi_T(s) \in N$ a round number; (iii) $\pi_R(s, \bar{\tau}) \in R$ a response time; and (iv) $\pi_s(s, \bar{\tau}) \in R$ a sampling time ($\pi_s(s) = \pi_R(s, \bar{\tau})$).

### 4.3 Environment-Restricted Controllers

A controller $M$ is basically a nondeterministic machine parameterized by any behavior of its environment $E_M$. A controller $M$ has a state space of the form $S \times \mathbb{R}^w$, where $\mathbb{R}^w$ denotes the $m$ physical parameters that $M$ can observe. Likewise, $E_M$ has a state space of the form $\mathbb{R}^u \times \mathbb{R}^w$, where $\mathbb{R}^u$ is the observable part of $E_M$. For state $\bar{\tau} \in \mathbb{R}^u$ of $E_M$, let $\pi_O(\bar{\tau}) \in \mathbb{R}^u$ denote the observable part of $\bar{\tau}$.

The environment restriction $M \mid E_M$ is a normal machine (see Def. 1) with a combined state space $S \times \mathbb{R}^u$, recording "snapshots" of $E_M$’s states at times $iT - \epsilon$. A transition of $M \mid E_M$ from state $(s, \bar{\tau})$ to $(s', \bar{\tau}')$ corresponds to realizable trajectories $\bar{\tau}$ for its period $T$ with respect to $\pi_s(s)$ and $\pi_c(s')$ and the response duration $u_R = (c_M(i) + \pi_R(s) - (iT - \epsilon)$.

The controller $M$ performs a transition based on the observable physical state $\pi_O(\bar{\tau}(i))$ of $E_M$ sampled after the sampling duration $u_I = (c_M(i) + \pi_I(s)) - (iT - \epsilon)$.

**Definition 7.** The environment restriction of $M$ by $E_M$ with an interface $\pi$ is $M \mid E_M = (D_S, S \times \mathbb{R}^u, D_o, \delta_M, (\mathbb{R}, D_E))$.

Figure 5: Timeline for an environment-restricted controller with a local clock $c_M$, where the curved line represents the state of $E_M$, and the straight lines represent the discrete states of $M$. 

\[\int_{-\infty}^{\infty} f(x) \, dx = \int_{-\infty}^{0} f(x) \, dx + \int_{0}^{\infty} f(x) \, dx\]
The interface \( \pi_M \) is defined by the projection functions: (i) \( \pi_C(i, r_M, v_M) = r_M \); (ii) \( \pi_T(i, r_M, v_M) = i \) (the round number); (iii) \( \pi_I(i, r_M, v_M) = 1 \) ms (the sampling time); and (iv) \( \pi_R(i, r_M, v_M), g_M = 2 \) ms (the response time). Thus, the sampling duration is \( u_T = (c_M(i) + 1) - (i - 15 - \varepsilon) \) and the response duration is \( u_R = u_T \) for each round. For \( E_M = (\mathbb{R}, \times_M, \Lambda_M) \) in Example 1, its observable state is given by the function \( \pi_0(x_M) = x_M \).

The environment restriction of \( M \) by \( E \) is then defined as the machine \( M = (\mathbb{R}, N \times \mathbb{R}^2, \mathbb{R}, \delta_M, E_M) \), where \((\langle (g_M, i), r_M, v_M), ((i', r'_M, v'_M), v_M) \rangle \in \delta_M \) holds iff:

(i) for some realizable trajectory \( \tau \in R_{E_M}^{\tau} (r_M, r_M, u_R) \), \( v_M = \tau(0) \) and \( v_M = \tau(15) \); and (ii) \( M \)’s transition \((g_M, i, r_M, \tau(u_i)) \) and \((i', r'_M, v'_M), v_M) \in \delta_M \) holds.

**Example 3.** Consider the main controller \( M_{\text{Main}} \) to roll the aircraft toward the specified angle in Example 1. In each 60 ms round, beginning at \( c_{\text{Main}}(i) \in (i - 60 ms - e, i - 60 ms + e) \), \( M_{\text{Main}} \) receives a desired roll angle \( \phi \), and sends the new goal angle \((g_M, g_R)\). \( M_{\text{Main}} \) is specified as the typed machine \((\mathbb{R}^2, N \times \mathbb{R}^2, \mathbb{R}, \delta_{\text{Main}}, E_{\text{Main}}) \), where \((\langle (g_M, i), r_M, (i, \phi), (i'), r'_M, v'_M, v_M) \rangle \in \delta_{\text{Main}} \) holds iff:

(i) \( \phi = \tau(0) \) and \( \phi = \tau(10) \) for realizable trajectories \( \tilde{\tau} \in R_{E_{\text{Main}}}^{\phi} (*) \), and (ii) for \( \tilde{\tau} = (\tau_0, \tau_R, \tau_L, \tau_{\text{Spec}}) \), \( ((g_M, r_M), (i, \phi), (i'), r'_M, v'_M, v_M) \in \delta_{\text{Main}} \).

4.4 Hybrid PALs: PALS Synchronous Models

The synchronous model in Hybrid PALS is specified as a multirate ensemble \( \mathcal{E} \) and the physical environments of subcomponents, where physical correlations between those environments are specified as time-invariant constraints.

**Definition 8.** A hybrid multirate ensemble \( \mathcal{E} \) is composed of: (i) \( \mathcal{E} \) a multirate ensemble, (ii) a family of interface functions \( \Pi = \{\pi_j\}_{j \in J_{\text{Env} \cup \text{F}}} \), and (iii) a family of local physical environments \( E = \{E_M\}_{j \in J_{\text{Env} \cup \text{F}}} \) with \((\forall \psi) \psi \) the time-invariant constraints (shown in Fig. 6).

**Example 4.** For the simple CPS controller in Example 1, \( E_{\text{Env}} \) is a multirate ensemble of the main controller \( M_{\text{Main}} \) and the subcontrollers \( M_I \) and \( M_R \), where rate(Main) = 1 and rate(L) = rate(R) = 4. The machines \( \{M_{\text{Main}}, M_I, M_R\} \), interfaces \( \Pi = \{\pi_{\text{Main}}, \pi_I, \pi_R\} \), and physical environments \( \{E_{\text{Main}}, E_I, E_R\} \) are defined in Examples 2-3. The network connections are shown in Fig. 4. The time-invariant constraint \((\forall \psi) \psi \equiv (\forall \psi) (\xi_L(t) = x_L(t)) \wedge (\xi_R(t) = x_R(t)) \) specifies the continuous physical connections.

A hybrid ensemble \( \mathcal{E} \) is induced by a normal multirate ensemble \( \mathcal{E} \) composed of the environment restrictions \( \{E_{J} \} \in J_{\text{Env} \cup \text{F}} \), which disregards the time-invariant constraints \((\forall \psi) \psi \). The behaviors of \( \mathcal{E} \) \( \models \psi \) are a subset of the behaviors of \( \mathcal{E} \models \psi \), namely, the behaviors restricted by \((\forall \psi) \psi \).

As mentioned, a transition of a (decelerated) environment-restricted machine \( M_J \models E_M \) corresponds to realizable trajectories \( \tilde{\tau} \) in a time interval \([\tau - \epsilon, (i + 1)T - \epsilon] \) for a global period \( T \). Hence, a lockstep composition of such transitions whose realizable trajectories \( \tilde{\tau} \) also satisfy the time-invariant constraints \((\forall \psi) \psi \) gives a transition of the synchronous composition \( \mathcal{E} \models \psi \).

4.5 Hybrid PALS Distributed Models

Hybrid PALS maps a hybrid ensemble \( \mathcal{E} \) \( \models \psi \) to the distributed hybrid system \( \mathcal{M}(\mathcal{E}, \Gamma) \) \( \models \psi \), together with PALS bounds \( \Gamma \); i.e., \( \mathcal{E} \models \psi \) \( \Rightarrow \mathcal{M}(\mathcal{E}, \Gamma) \models \psi \).

The distributed components in \( \mathcal{M}(\mathcal{E}, \Gamma) \) \( \models \psi \) are exactly the same as the wrapper hierarchies of Fig. 2 in \( \mathcal{M}(\mathcal{E}, \Gamma) \). But the controllers in \( \mathcal{M}(\mathcal{E}, \Gamma) \) \( \models \psi \) also interact with their physical environments in \( \mathcal{E} \), according to the sampling and response timing policies \( \Gamma \) to determine sensor sampling timing \( t_\tau \) and actuator response timing \( t_R \).

The behaviors of the Hybrid PALS distributed system \( \mathcal{M}(\mathcal{E}, \Gamma) \) \( \models \psi \) are the subset of those of the PALS distributed system \( \mathcal{M}(\mathcal{E}, \Gamma) \), restricted by the physical environments and the time-invariant constraints in \( \mathcal{E} \). The continuous dynamics of \( \mathcal{M}(\mathcal{E}, \Gamma) \) \( \models \psi \) are “completely” decided by the controllers, their physical environments, the timing policies, and the local clocks of the controllers.

More precisely, consider a normal ensemble \( \mathcal{E} \) \( \models \psi \) above, induced by a hybrid ensemble \( \mathcal{E}_\rho \) \( \models \psi \), and composed of the environment-restricted controllers \( \{M_J \models E_{J}\}_{j \in J_{\text{Env} \cup \text{F}}} \). A big-step transition is defined from one stable state at time \( t - e \) to another stable state at \( (i + 1)T - e \) for the system \( \mathcal{M}(\mathcal{E}, \Gamma) \) \( \models \psi \), as explained in Section 3.2. For such time intervals \([t - \epsilon, (i + 1)T - \epsilon] \), each \( M_J \models E_{J} \) provides (k-step) realizable trajectories \( \tilde{\tau}_j \), based on round numbers, control commands, sampling timings, and response timings.

The behaviors of \( \mathcal{M}(\mathcal{E}, \Gamma) \) \( \models \psi \) are the behaviors of \( \mathcal{M}(\mathcal{E}, \Gamma) \) \( \models \psi \) that are restricted by the time-invariant constraints \( \Gamma \). Big-step transitions of \( \mathcal{M}(\mathcal{E}, \Gamma) \) \( \models \psi \) are therefore exactly those of \( \mathcal{M}(\mathcal{E}, \Gamma) \) \( \models \psi \) whose associated trajectories \( \tilde{\tau}_j \) satisfy the time-invariant constraints \((\forall \psi) \psi \).

The correctness of Hybrid PALS follows from the fact that each physical measurement and physical activation happens at the same time in both \( \mathcal{E} \) \( \models \psi \) and \( \mathcal{M}(\mathcal{E}, \Gamma) \) \( \models \psi \) with the same timing policies \( \Gamma \) (see (4) for more details).

**Theorem 2.** The relation \( \sim_{\text{obs}} \) \( \text{sync} \) is a bisimulation between the transition system \( ts(M_{\mathcal{E}}) \) and the big-step transition system induced by \( \mathcal{M}(\mathcal{E}, \Gamma) \) \( \models \psi \), exhibiting the exactly same set of realizable trajectories.

**Proof Sketch.** Suppose that there exists a transition \( s \longrightarrow \mathcal{E}_\rho \) \( \models \psi \) \( \mathcal{E}_\rho \) \( \models \psi \) \( \mathcal{E}_\rho \) \( \models \psi \) \( \mathcal{E}_\rho \) \( \models \psi \) \( \mathcal{E}_\rho \) \( \models \psi \) \( \mathcal{E}_\rho \) \( \models \psi \) \( \mathcal{E}_\rho \) \( \models \psi \), and \( (\sim_{\text{obs}} \ \text{sync}) \) \( \models \psi \) for a stable
state $C$ of $MA(E_T, \Gamma) \upharpoonright \Gamma E$. By definition, there exists $s \xrightarrow{\tau \notin \Gamma E} s'$ of $MT_{\Gamma E}$ with some realizable trajectories $\bar{\tau}$ that satisfy the time-invariant constraints $(\forall t)(\forall \psi)$ for the induced ensemble $E_T \upharpoonright \Gamma E$. By Theorem 1, $(\sim obs; \text{sync})$ is a bisimulation between the transition systems $TS_{MT_{\Gamma E}}$ and $(Stable(MA(E_T, \Gamma) \upharpoonright \Gamma E), \rightarrow)$. Therefore, for some stable state $C'$, there is a big-step transition $C \rightarrow_{\tau} C'$ in $MA(E_T, \Gamma) \upharpoonright \Gamma E$, such that $s \xrightarrow{\tau} s'$ and $C \rightarrow_{\tau} C'$ involve exactly the same machine states and inputs. By construction, round numbers, control commands, sampling timings, and response timings all depend on machine states and inputs. Therefore, the trajectories $\bar{\tau}$, which satisfy $(\forall t)(\forall \psi)$, are also realizable for $C \rightarrow_{\tau} C'$, and there is a big-step transition $C \rightarrow_{\tau} C'$ by $MA(E_T, \Gamma) \upharpoonright \Gamma E$. The other direction is similar. □

5. HYBRID PALS MODELS IN SMT

Theorem 2 implies that analyzing $MA(E_T, \Gamma) \upharpoonright \Gamma E$ can be reduced to the much simpler problem of analyzing $MA(E_T \upharpoonright \Gamma E)$, which abstracts from asynchronous communication, network delays, execution times, message buffering, etc. This section shows how analysis problems for a hybrid ensemble $E_T \upharpoonright \Gamma E$ can be encoded as formulas over the real numbers and ODEs. We symbolically encode all possible local clocks to deal with clock skew. Standard formal analysis problems for hybrid systems, such as bounded reachability, inductive reasoning, and compositional assume-guarantee reasoning, are encoded as logical formulas. The satisfiability of such formulas can be decided by $\delta$-complete SMT solving [8, 10] up to a given precision $\delta > 0$. $\delta$-complete SMT solving for a formula $\phi$ returns false if it is unsatisfiable, and returns true if its syntactic numerical perturbation of $\phi$ by $\delta$ is satisfiable. 1

5.1 Encoding Hybrid PALS Models

5.1.1 Encoding Environment-Restricted Controllers

A controller $M$ can be expressed as a formula of the form $\phi_M(\vec{i}, \vec{y}, \vec{y}', \vec{a}, \vec{r})$, with variables $\vec{i}$, $\vec{y}$, $\vec{y}'$, and $\vec{a}$ denoting input, output, respectively, and in such a way that $\phi_M(\vec{i}, \vec{r}) \iff (\vec{i}, \vec{r}) \in \Delta_M$.

Example 5. For an aileron subcontroller $M$ in Example 2, the formula $\phi_M(y_{low}, y_{high}, y, y', \vec{a}, \vec{r}, v, u, \vec{y}, \vec{y}_0) \equiv (y'_{low} = (y_{low} - y_{high})/15 \land y = y_{low} \land y' = y_{low} + 1)$. Likewise for the main controller $M_{Main}$ in Example 3 is $\phi_{Main}(y_{high}, y_{low}, \vec{y}, \vec{r}, v, u, \vec{y}_0) \iff (y_{low} = 0.3(y_{low} - y_{low}) \land y_{low} = -y_{low} \land y = y_{low} \land y' = y_{low} + 1)$.

A physical environment $E_S$ is encoded as a formula of the form $\phi_{E_S}(\vec{a}, \vec{v}, u, \vec{r}, \vec{a})$, with: unary function symbols $\vec{a}$ denoting the trajectories of $E_S$'s physical parameters $\vec{x}$, and variables $\vec{a}$, $\vec{v}$, and $u$ denoting, respectively, control commands, and the initial values of $\vec{a}$ at time $t_0$, the times at the beginning and the end of the trajectory duration, where $\phi_{E_S}(\vec{a}, \vec{v}, u, \vec{r}, \vec{a}) \iff ((\vec{a}, \vec{v}, u, \vec{r}, \vec{a}) \in \Delta_{E_S})$.

If the continuous dynamics of $\vec{x}$ is specified as a system of ODEs $\vec{x}' = F_S(\vec{x}, t)$ for a control command $\vec{a}$ and an interval $[u_0, u_1]$, then $\phi_{E_S}$ includes universal quantification over time along with solutions of the ODEs, for example: $\forall t (\frac{\partial}{\partial t} (\vec{x}(t)) = F_S(\vec{x}(t), t))$.

1If $\phi \equiv (x > 3) \land (y \equiv z \lor y' \equiv z \lor (y - z \geq \delta))$, then its syntactic numerical perturbation by $\delta$ is $(x - 3 > -\delta) \land (y - z \geq -\delta) \land (y' - z \geq -\delta)$.

Example 6. For an aileron subcontroller $M$ in Example 1, the formula $\phi_{E_M}(y_{low}, y_{high}, y, u, \vec{r}, \vec{a}, \vec{r}) \equiv (\forall t \in [0, y_{low}], \tau_M(t) = y_{low} + \int_0^t \tau_M(u) \, du)$.

For the main controller $M_{Main}$, if $y_{low} = 0$, then the formula $\phi_{E_M}(y_{low}, y_{high}, y, u, \vec{r}, \vec{a}, \vec{r}) \equiv (\forall t \in [0, y_{low}], \tau_M(t) = y_{low} + \int_0^t \tau_M(u) \, du)$.

The encoding of an environment restriction $M \upharpoonright \Gamma E$ has the form $\phi_{M_{E_S}}(\vec{i}, \vec{y}, \vec{r}, \vec{a}, \vec{r})$, with unary function symbols $\vec{a}$ denoting $E_S$'s trajectories, and variables: (i) $\vec{i}$ denoting input, (ii) $\vec{y}$ denoting state at the beginning of the round (at time $\tau - \epsilon$), (iii) $\vec{y}'$ denoting a state at the end of the round (at time $(\tau + 1)T - \epsilon$), and (iv) $\vec{r}$ denoting output, given a period $T$ and a round number $i$.

The values of sampling duration $u_i = (c_M(i + 1)T - (i - 1)\epsilon)$ and response duration $u_R = (c_M(i) + i)T - (i - 1)\epsilon$ are unknown, due to clock skews. Since $i\epsilon - c_M(i)T < i\epsilon - c_M(i + 1)T - \epsilon$, we represent those times as formulas $t_i \leq u_i < t_i + 2\epsilon$ and $t_R < u_R < t_R + 2\epsilon$, so that $\phi_{M_{E_S}}(i, s, \vec{v} = \vec{i}, \vec{r}, \vec{a})$ iff $(\vec{i}, \vec{v}, \vec{r})$, $(\vec{s}, \vec{v})$, $(\vec{r}, \vec{a})$ $\in \Delta_{E_S}$ for some local clock $c_{E_S}$.

For an environment restriction $M \upharpoonright \Gamma E$ in Example 2, the formula $\phi_{E_M}(y_{low}, y_{high}, y, u, \vec{r}, \vec{a}, \vec{r}) \equiv (\forall t \in [0, y_{low}], \tau_M(t) = y_{low} + \int_0^t \tau_M(u) \, du)$.

Example 7. For $M \upharpoonright \Gamma E$ in Example 2, the formula $\phi_{E_M}(y_{low}, y_{high}, y, u_R, \vec{r}, \vec{a}, \vec{r}) \equiv (\forall t \in [0, y_{low}], \tau_M(t) = y_{low} + \int_0^t \tau_M(u) \, du)$.

5.1.2 Encoding Hybrid Ensembles

Recall that all machines in a synchronous composition $M_{FS}$ perform their transitions in lockstep; for a fast machine $f$, $k = rate(f)$ transitions in a global round. The encoding $\phi_{M_{E_S}}^{(t_{max})}$ of the $k$-step deceleration of an environment restriction $M \upharpoonright \Gamma E$ is given by sequentially composing the $k$ formulas $\phi_{M_{E_S}}^{(t_{max})}$ for the $k$ subintervals $[i\epsilon + (n - 1)T/k, i\epsilon + nT/k]$ for $n = 1, \ldots, k$.

The encoding $\phi_{enw}$ of $E_T$'s wiring diagram is a conjunction of equalities between variables for input and output ports. Each equality corresponds to a connection in $E_T$ (together with an input adaptor for machines with different rates). Since feedback outputs become input of their destinations in the next step, we use a separate set of variables for such output ports connected to machines in $E_T$.
A hybrid ensemble $E_T \mid_{I} E$ of typed machines $\{M_j\}_{i \in J}$, physical environments $\{E_{M_j}\}_{i \in J}$, for $J = J_S \cup J_F$, and the time-invariant constraint $(\forall t. \emptyset)$ is encoded as a formula $\phi_{E_T \mid_{I} E}(i, \bar{y}, \bar{v}, \bar{y}, \bar{v}) \in J \mid \forall t. (i, \bar{y}, \bar{v}, \bar{y}, \bar{v}) \in J \mid \bar{t} \in \bar{t}$ as: 

$$\exists \{t_i, o_i\}_{i \in J} \land \bigwedge_{f \in J_F} (\phi(T \rightarrow E_{M_j} \mid_{I} E_{M_j} \mid \forall t. (i, \bar{y}, \bar{v}, \bar{y}, \bar{v}) \in J \mid \bar{t} \in \bar{t}) \land \phi_{core}(i, \bar{t}, \{\bar{t}_i, \bar{o}_i, \bar{f}_j\})_{i \in J}) \land (\forall t. \emptyset)$$

with unary function symbols $\bar{t}$ denoting trajectories for $E_{M_j}$, and variables $(\bar{y}_i, \bar{v}_i)$, $\bar{f}_j$, $(\bar{y}_i, \bar{v}_i)$, and $\bar{f}_j$ denoting, respectively, the state of $M_j \mid_{I} E_{M_j}$ at the beginning of the round, the feedback outputs from the previous round, the state of $M_j \mid_{I} E_{M_j}$ at the end of the round, and the feedback outputs for the next round. The variable $\bar{t}$ denotes ensemble inputs, and $\bar{t}$ denotes ensemble outputs.

By construction, a formula $\phi_{E_T \mid_{I} E}$ is satisfiable iff there is a corresponding translation of the synchronous composition $M_{E_T \mid_{I} E}$ from $\bar{t}T - \epsilon$ to $(i + 1)\bar{t}T - \epsilon$ for some local clocks. Hence, by the bisimulation equivalence (Theorem 2):

**Theorem 3.** The formula $\phi_{E_T \mid_{I} E}$ is satisfiable iff there exists a corresponding stable transition for some local clocks in a distributed hybrid model $M_{A}(E_T, \Gamma) \mid_{I} E$.

**Example 8.** The hybrid ensemble $E_{00} \mid_{I} E$ in Example 4 is encoded as the formula $\phi_{E_{00} \mid_{I} E}$, the conjunction of the following formulas: (i) for the main controller:

$$\phi_{M_0 \mid_{I} E_{M_0}}(y_{0, \bar{i}}, y_{0, \bar{0}}, y_{l, \bar{l}}, y_{0, \bar{0}}, y_{l, \bar{l}}, \bar{t})$$

with $\bar{y} = (y_{e_1}, y_{e_2}, y_{e_3}, y_{e_4}, y_{e_5}, y_{e_6})$ and $\bar{t} = (t, t, t, t, t, t)$; (ii) for the subcontrollers:

$$\phi_{M_{l} \mid_{I} E_{M_{l}}} \times 4(y_{0, \bar{0}}, y_{l, \bar{l}}, y_{0, \bar{0}}, y_{l, \bar{l}})$$

with $\bar{y}_{0, \bar{0}} = (y_{0, \bar{0}}, y_{0, \bar{0}}, y_{0, \bar{0}}, y_{0, \bar{0}})$, and for $m \in \{L, R\}$, $\bar{y}_{0, \bar{0}} = (y_{0, \bar{0}}, y_{0, \bar{0}}, y_{0, \bar{0}}, y_{0, \bar{0}})$; (iii) for the wiring diagram:

$$y_{0, \bar{0}} = f_{port} \land f_{port} = y_{0, \bar{0}} \land (y_{0, \bar{0}} = y_{0, \bar{0}} \land f_{port} = y_{0, \bar{0}} \land f_{port} = y_{0, \bar{0}} \land f_{port} = y_{0, \bar{0}})$$

with variables $f_{port}$ denoting a feedback output from the previous step, and $f_{port}$ denoting one for the next step; and finally, (iv) for the time-invariant equality constraint $(\forall t. \bar{t}_L(t) = \bar{t}_R(t) \land \bar{t}_R(t) = \bar{t}_L(t))$.

**5.2 Inductive Reasoning**

For unbounded time verification, we encode an inductive proof of a safety property $safe(y, \bar{t}(t))$ as a logical formula by using an inductive condition for $M_{E_T \mid_{I} E}$’s synchronous transitions, which implies the safety property. An inductive invariant consists of two formulas: $ind_d(y)$ for state variables $y$, and $\forall t \in [0, T]. ind_c(\bar{t}(t))$ for trajectories $\bar{t}$.

**Definition 9.** Bounded reachability of $M_{E_T \mid_{I} E}$ up to $n$ rounds for a safety property $safe(y, \bar{t}(t))$, an initial condition $init(y)$, and an input constraint $in(\bar{t})$ is encoded by:

$$\exists \bar{y}_0, (\bar{y}_k, \bar{t}_k, \bar{o}_k, t_k)_{k=1}^n. \quad \forall k=1^n. safe(y_k, \bar{t}_k)$$

$$\land \bigwedge_{k=1}^n \left( \phi_{E_T \mid_{I} E}(\bar{y}_k, \bar{t}_k-1, \bar{o}_k, \bar{t}_k) \land in(\bar{t}_k) \right)$$

Some initial state $y_0$ satisfies the init condition, and then $M_{E_T \mid_{I} E}$ performs $n$ steps of synchronous transitions, each of which is from some state $y_{k-1}$ to $y_k$ using trajectories $\bar{t}_k$ of duration $T$ with some input $\bar{t}_k$ satisfying the input constraint $in$. $M_{E_T \mid_{I} E}$ has bounded counterexamples if some state $(y_k, \bar{t}_k(t_k))$ at some time $t_k$ violates the safety $safe$.

**5.2.3 Compositional Reasoning**

We code a divide-and-conquer proof to verify a safety property using standard assume-guarantee reasoning. It is very useful for dealing with the state explosion problem. In $M_{E_T \mid_{I} E}$, each component $M_j \mid_{I} E_{M_j}$ performs a transition based on its input $t_i$ and trajectories $\bar{t}_j$ that are restricted by time-invariant constraints. Hence, we use an input condition $c_{in}(t_i, \bar{t}_j(t))$ and an output condition $c_{out}(t_j, \bar{t}_j(t))$, which satisfy necessary constraints for compositional reasoning: (i) assuming an input condition $c_{in}(t_i, \bar{t}_j(t))$, if a transition is taken, then the output condition $c_{out}(t_j, \bar{t}_j(t))$ holds; and (ii) the collection of the output conditions $\{c_{out}(t_j, \bar{t}_j(t))\}_j$ implies each input condition $c_{in}(t_i, \bar{t}_j(t))$. Let $M_{\bar{D}}$ denote its decelerated version $(M_j \mid_{I} E_{M_j})^{\bar{D}}(\bar{t})$. $\bar{D}$ is a key problem is finding such an inductive invariant for $M_{E_T \mid_{I} E}$, but providing general solutions for this problem is beyond the scope of this paper.
Definition 11. For each component $j$ in a hybrid ensemble $E_T \upharpoonright [0,T]$, consider a safety property $safef \left( \vec{y}_j, \vec{\tau}_j(t) \right)$, an input constraint $\text{init}_j \left( \vec{\tau}_j \right)$ for input from $E_T$’s interface, and an initial condition $\text{init}_j \left( \vec{y}_j \right)$. I/O conditions are given by:

\[
\forall t. \, c_{in} \left( \vec{\tau}_j(t) \right) = \left( c_{in} \left( \vec{\tau}_j \right) \wedge \forall t \in [0,T]. \, c_{out} \left( \vec{\tau}_j(t) \right) \right)
\]

\[
\forall t. \, c_{out} \left( \vec{\tau}_j(t) \right) = \left( c_{out} \left( \vec{\tau}_j \right) \wedge \forall t \in [0,T]. \, c_{in} \left( \vec{\tau}_j(t) \right) \right)
\]

that satisfy the necessary constraints for a compositional reasoning of the synchronous composition $E_T \upharpoonright [0,T]$:

- $\forall t. \, c_{in} \left( \vec{\tau}_j(t) \right)$ $\Rightarrow$ $\forall t \in [0,T]. \, c_{in} \left( \vec{\tau}_j(t) \right)$

- $\forall t \in [0,T]. \, c_{out} \left( \vec{\tau}_j(t) \right)$ $\Rightarrow$ $\forall t \in [0,T]. \, c_{out} \left( \vec{\tau}_j(t) \right)$

Both bounded reachability and inductive reasoning can be then separately performed for each component by also assuming input conditions for individual components. A compositional bounded reachability problem up to $n \in \mathbb{N}$ rounds for component $j$ is encoded by:

\[
\exists \hat{y}_0, \left( \vec{y}_j \in \mathbb{R}^n \right), \vec{\tau}_k, t_k \in [0, T] \wedge \forall k \leq n. \text{init}_j \left( \hat{y}_k \right) \wedge \left( \vec{\tau}_k, t_k \right) = \left( \vec{\tau}_k, t_k \right)
\]

\[
\wedge \forall k \leq n. \left( \vec{\tau}_k \right) \in \left( \vec{\tau}_k, t_k \right) \wedge \forall k \leq n. \text{ind}_j \left( \vec{\tau}_k \right)
\]

Where the input condition $\forall t \in [0,T]. \, c_{in} \left( \vec{\tau}_j(t) \right)$ is also assumed for each step in addition to Definition 9.

Likewise, a compositional inductive reasoning problem of $safef \left( \vec{y}_j, \vec{\tau}_j(t) \right)$ for component $j$ with an inductive condition $\text{ind}_j \left( \vec{\tau}_j \right)$ $\wedge \forall t \in [0,T]. \, c_{out} \left( \vec{\tau}_j(t) \right)$ can be encoded by:

- $\forall \vec{y}_j, \text{init}_j \left( \vec{y}_j \right) \Rightarrow \text{ind}_j \left( \vec{y}_j \right)$

- $\forall \vec{y}_j, \vec{\tau}_j, \vec{\tau}_j, \vec{\tau}_j \left( \vec{\tau}_j(t) \right)$ $\Rightarrow$ $\text{ind}_j \left( \vec{\tau}_j \right)$

- $\forall \vec{y}_j, \forall t. \, \text{ind}_j \left( \vec{y}_j \right) \wedge \text{ind}_j \left( \vec{\tau}_j \right) \Rightarrow \text{safe} \left( \vec{y}_j, \vec{\tau}_j(t) \right)$

The formulas for compositional reasoning can also be proved by checking the unsatisfiability of their negated versions.

5.3 Removing Universal Quantification

The formulas encoding Hybrid PALS models may contain universal quantification over uninterpreted functions on the real numbers, such as time-invariant constraints $\forall t. \, \psi$ or formulas of the form $\forall t \in [u_0, u_1]. \, \varphi(t) = \varphi + \int_0^t F_0(t) \varphi(t) \, dt$. The above quantifiers are not directly supported by current state-of-the-art SMT techniques. This section explains how such universal quantification can be removed from the formulas.

We restrict our attention to time-invariant constraints with only equality terms, since continuous constraints typically can be expressed using only equalities (e.g., Example 1). Equality constraints, such as $x_1(t) = x_2(t)$, can be removed from the formula by replacing one side with the other, e.g., by replacing each function symbol $x_1$ with $x_2$. From now on we assume that time-invariant equality constraints have been removed from the formula in this way. 3Providing general solutions for how to find I/O conditions for $E_T \upharpoonright [0,T]$ is beyond the scope of this paper.

Now consider universally quantified formulas of the form $\forall t \in [u_0, u_1]. \, \varphi(t) = \varphi + \int_0^t F_0(t) \varphi(t) \, dt$. Recall that the term $F_0(t) \varphi(t)$ may include “uninterpreted” functions whose meaning is defined by other components. We assign to a time interval $\left[ u_0, u_1 \right]$ a global round such a “partial” ODE system $\frac{d\varphi}{dt} = F_0(x, t)$. If every component $j$ assigns its partial ODE system $\frac{d\varphi_j}{dt} = F_0_j(x_j(t), t)$ to its interval $\left[ u_0, u_1 \right]$, then a complete ODE system $\left\{ \frac{d\varphi_j}{dt} = F_0_j(x_j(t), t) \right\}_j$, which contains no uninterpreted functions, can be constructed for the common interval $\left[ u_0, u_1 \right]$, provided that variables are renamed by the equality time-invariant constraints.

Example 9. The physical environment $E_{Main}$ of the main controller in Example 1 involves the formula

\[
\forall t \in [0,60]. \, \left[ \tau_s(t) = \frac{\tau_p(t)}{\tau_p(t)} + \int_0^t \left( c(\tau_R(t) - \tau_L(t)) \right) dt \right]
\]

including two uninterpreted function symbols $\tau_s$ and $\tau_R$. Consider two logical formulas: for the left subcontroller, $\forall t \in [u_0, u_1]. \, \tau_s(t) = \tau_p + \int_0^\tau \frac{\tau_p(t)}{\tau_p(t)} dt$, and for the right subcontroller, $\forall t \in [u_0, u_1]. \, \tau_s(t) = \tau_p + \int_0^\tau \frac{\tau_p(t)}{\tau_p(t)} dt$. For the common interval $\left[ u_0, u_1 \right]$, the complete ODE system is:

\[
\left[ \begin{array}{l}
\tau_s(t) \\
\tau_s(t) \\
\tau_s(t) \\
\tau_s(t) \\
\tau_s(t)
\end{array} \right] = \left[ \begin{array}{l}
\frac{\tau_p(t)}{\tau_p(t)} \\
\frac{\tau_p(t)}{\tau_p(t)} \\
\frac{\tau_p(t)}{\tau_p(t)} \\
\frac{\tau_p(t)}{\tau_p(t)} \\
\frac{\tau_p(t)}{\tau_p(t)}
\end{array} \right] \int_0^\tau \left( c(\tau_R(t) - \tau_L(t)) \right) dt
\]

This system indicates a period that the right subcontroller has responded (with the new rate $rate_p'$) but the left one has not responded yet (due to the clock skews).

More precisely, a global period $[0,T]$ for one round of an ensemble $E_T \upharpoonright [0,T]$ is divided into $N$ contiguous subintervals $[0,t_1], [t_1,t_2], [t_2,t_3], \ldots, [t_{n-1},T]$. Each interval denotes a single time segment to which a complete system of ODEs is assigned. The number $N$ is determined by the total number of interval assignments in one round, namely, a number of ODE subformulas $\forall t \in [u_0, u_1]. \, \varphi(t) = \varphi + \int_0^t F_0(t) \varphi(t) \, dt$. We have verified safety properties using inductive and compositional SMT encodings for any possible set of local clocks with maximal clock skew $\epsilon$. We have applied the dReal SMT solver [9] to check the satisfiability of the SMT formulas up to a given precision $\delta > 0$ (which is decidable for nonlinear hybrid systems [8, 10]). All experiments were conducted on an Intel Xeon 2.0 GHz with 64 GB memory. The case studies and the experimental results are available at http://dreal.github.io/benchmarks/networks.

6. CASE STUDIES

This section gives an overview of some case studies that use our methodology to verify virtually synchronous distributed hybrid systems. All the case studies involve nonlinear ODEs and continuous interactions between distributed components. They also take into account asynchronous communication, network delays, clock skews, execution times, etc. Owing to the bisimulation equivalence, we can analyze the simpler synchronous models $E_T \upharpoonright [0,T]$ instead of analyzing the distributed hybrid models $MA(E_T, T) \upharpoonright [0,T]$.

We have verified safety properties using inductive and compositional SMT encodings for any possible set of local clocks with maximal clock skew $\epsilon$. We have applied the dReal SMT solver [9] to check the satisfiability of the SMT formulas up to a given precision $\delta > 0$ (which is decidable for nonlinear hybrid systems [8, 10]). All experiments were conducted on an Intel Xeon 2.0 GHz with 64 GB memory. The case studies and the experimental results are available at http://dreal.github.io/benchmarks/networks.
6.1 Turning an Airplane

We consider a multirate virtually synchronous distributed controller to turn an airplane (adapted from [2]). This is a more elaborate version of Example 1. To make a turn, an aircraft rolls towards the direction of the turn by moving its ailerons. The rolling causes a yawing moment in the opposite direction, called adverse yaw, which is countered by using its rudder (a flap attached to the vertical stabilizer). The subcontrollers for the ailerons and the rudder operate at different rates, and the main controller orchestrates them to achieve a smooth turn, as illustrated in Fig. 7. The desired safety property is that the yaw angle $\beta$ is always close to 0.

Each subcontroller $M$ gradually moves its surface towards the goal angle $goal_{M}$ specified by the main controller $M_{Main}$, as explained in Example 1. In each round, $M$ receives $goal_{M}$ from $M_{Main}$, determines the moving rate $rate_{M}$ based on $goal_{M}$ and the current sampled value $v_{M}$ of the angle $\alpha_{M}$, and sends back $v_{M}$ to $M_{Main}$. The local environment $E_{M}$ specifies the dynamics of $\alpha_{M}$ by the ODE $\alpha_{M} = rate_{M}$. The main controller $M_{Main}$ determines the goal angles for the subcontrollers to make a coordinated turn. In each round, $M_{Main}$ receives a desired direction $goal_{\psi}$ (from the pilot) and the angles $(v_{L}, v_{V}, v_{R})$ from the subcontrollers, and sends back the new goals $(goal_{L}, goal_{V}, goal_{R})$, based on the current sampled position values $(v_{L}, v_{V}, v_{R})$ of the direction angle $\psi$, the roll angle $\phi$, and the yaw angle $\beta$. We use a simple control logic to decide the new goals based on the current position angles, namely, by using some function $(goal_{L}, goal_{V}, goal_{R}) = f_{Main}(v_{\psi}, v_{\phi}, v_{\beta})$.

The environment $E_{Main}$ specifies the lateral dynamics of an aircraft as the nonlinear ODEs (depicted in Fig. 8):

$$\dot{\beta} = Y_{\zeta_{L},\zeta_{V},\zeta_{R}} \cdot m/V - r + (g/V) \cos \beta \sin \phi,$$
$$\dot{\phi} = p,$$
$$\dot{\psi} = (g/V) \tan \phi,$$
$$\dot{p} = (c_{1} r + c_{2} p) \cdot r \tan \phi + c_{3} L_{\zeta_{L},\zeta_{V},\zeta_{R},\beta} + c_{4} N_{\zeta_{L},\zeta_{V},\zeta_{R},\beta},$$
$$\dot{r} = (c_{3} p - c_{2} r) \cdot r \tan \phi + c_{4} L_{\zeta_{L},\zeta_{V},\zeta_{R},\beta} + c_{9} N_{\zeta_{L},\zeta_{V},\zeta_{R},\beta},$$

where $p$ is the rolling moment, $r$ is the yawing moment, and $Y_{\zeta_{L},\zeta_{V},\zeta_{R},\beta}$, $L_{\zeta_{L},\zeta_{V},\zeta_{R},\beta}$, and $N_{\zeta_{L},\zeta_{V},\zeta_{R},\beta}$ are (linear) functions of the control angles $(\zeta_{L}, \zeta_{V}, \zeta_{R})$ and $\beta$.

The physical environment $E_{Main}$ clearly depends on the subcontrollers’ physical environments. Each control angle $\zeta_{M}$ in $E_{Main}$ must be the same as the corresponding surface angle $\alpha_{M}$, but the ODEs of the subcontrollers cannot be directly “plugged” into $E_{Main}$ because the main controller and the subcontrollers have different periods with local clock skew.

The continuous connections between the physical environments are specified by the time-invariant constraint: \( \forall t \in [0, T], (\zeta(t) = \alpha(t) \wedge \zeta_{V}(t) = \alpha_{V}(t) \wedge \zeta_{R}(t) = \alpha_{R}(t)) \).

We first performed bounded reachability analysis to verify the safety property $\forall t \in [0, T], abs(\beta(t)) < 0.2$, where all state variables are initially 0° and the goal direction from the pilot is fixed (e.g., 30°). In the analysis, we assume the sampling time $t_s = 0$ ms for every controller, the response time $t_{R} = 3$ ms for every subcontroller (the main controller has no actuator), and the maximal clock skew $\epsilon = 0.2$ ms. For bound $k = 10$, the analysis took 16 hours using dReal with precision $\delta = 0.0001$, which is quite slow due to complex nonlinear ODEs, nontrivial discrete controls, etc.

Therefore, we have applied compositional reasoning to conduct a bounded reachability analysis in a compositional way. We first show that each subcontroller cannot abruptly change its surface angle towards its goal direction in one round, so that the change is always less than a certain value.\(^5\)

Next, assuming that a subcontroller cannot abruptly move its surface, we perform a bounded reachability analysis only for the main controller using the same initial condition. For bound $k = 20$, using dReal with precision $\delta = 0.0001$, the compositional bounded reachability analysis for the safety property $\forall t \in [0, T], abs(\beta(t)) < 0.2$ took 2 minutes.

6.2 Networked Water Tank Controllers

In this benchmark, adapted from [16], a number of water tanks are connected by pipes as shown in Fig. 9. The water level in each tank is controlled by a pump in the tank, and depends on the pump’s mode $m \in \{m_{on}, m_{off}\}$ and the water level of the input tank. The water level $x_i$ of tank $i$ changes according to the nonlinear ODEs:

$$A_{i} x_{i} = \begin{cases} (q_{i} + a \sqrt{2g \sqrt{x_{i-1}}}) - b \sqrt{2g \sqrt{x_{i}}} & \text{if} \ m_{i} = m_{on} \\ a \sqrt{2g \sqrt{x_{i-1}}} - b \sqrt{2g \sqrt{x_{i}}} & \text{if} \ m_{i} = m_{off} \end{cases}$$

We set $x_0 = 0$ for the leftmost tank 1. Each pipe controller performs its transitions according to its local clock and sets the pump to on if $x_i \leq L_{min}$ and to off if $x_i > L_{M}$. The desired safety property is that each water level $x_i$ is in the range $I = [L_{min} - \eta, L_{M} + \eta]$, expressed as $(\forall t) x_i(t) \in I$.

We have verified the safety property for any number of connected water tanks for unbounded time with respect to clock skew using compositional inductive reasoning. First, assuming that the input water level $x_{i-1}$ is in $I$, we show that $x_i$ is in a tighter range $I' = [L_{min} - \eta', L_{M} + \eta']$ with $\eta' < \eta$ during any round $[0,T]$.\(^6\)

Next, assuming that the input level $x_{i-1}$ is in $I$, we show that $(\forall t) x_i(t) \in I$ is an inductive condition for one round (that is, $x_i(0) \in I$, $\forall t \in [0,E]$), and the desired safety property $x_i(t) \in I$ implies $x_i(t) \in I$.

\(^5\)E.g., the output condition for the left subcontroller is $c_{out}(x_1(t)) \equiv \forall t \in [0,T], abs(\alpha_{L}(t) - v_{L}) < \gamma$.

\(^6\)If the ODE conditions are $c_{in}(x_{i-1}(t)) \equiv \forall t \in [0,T], x_{i-1}(t) \in I$ and $c_{out}(x_i(t)) \equiv \forall t \in [0,T], x_i(t) \in I'$.
6.3 Networked Thermostat Controllers

A number of rooms are interconnected by open doors, as shown in Fig. 9. The temperature $x_i$ of each room $i$ is separately controlled by its own thermostat controller that turns the heater on and off. That is, $x_i$ depends on the heater's mode $m_i \in \{ m_{\text{on}}, m_{\text{off}} \}$ and the temperatures of the connected rooms, and changes according to the ODEs:

$$\dot{x}_i = \begin{cases} K_i (h_i - ((1 - 2c)x_i + cx_{i-1} + cx_{i+1})) & \text{if } m_i = m_{\text{on}} \\ -K_i((1 - 2c)x_i + cx_{i-1} + cx_{i+1}) & \text{if } m_i = m_{\text{off}} \end{cases}$$

In each transition, a controller of room $i$ turns on the heater if $x_i < T_m$, and turns it off if $x_i > T_M$. The safety property is that the temperature $x_i$ of each room is in a certain range $I = [T_m - \eta, T_M + \eta]$, expressed as $(\forall t) x_i(t) \in I$.

We have verified the desired safety property $(\forall t) x_i(t) \in I$ for any number of interconnected thermostat controllers for unbounded time, taking into account clock skews, by compositional inductive reasoning. Provided that both temperatures $x_{i-1}$ and $x_{i+1}$ of the connected rooms are in $I$, we show that $x_i$ is in a tighter range $I' = [T_m - \eta', T_M + \eta'] \subseteq I$ with $\eta' < \eta$ during one round. Then, assuming that both $x_{i-1}$ and $x_{i+1}$ are in $I$, we show that $(\forall t) x_i(t) \in I$ is an inductive condition for one round in a similar way to Section 6.2.

We have proved the safety property for any number of thermostats for maximal clock skew $\epsilon = 2$ ms, sampling time $t_I = 10$ ms, and response time $t_R = 200$ ms, using dReal with precision $\delta = 0.001$ (the analysis took 2.6 seconds). However, if $\epsilon = 20$ ms, then the compositional inductive condition $(\forall t) x_i(t) \in I$ is violated because the temperature rises for extra 20 ms and thus $x_i \notin I$ at the end of the round (the analysis took 0.56 seconds).

7. CONCLUDING REMARKS

We have presented general techniques for verifying virtually synchronous distributed hybrid systems, with asynchronous communication, imprecise local clocks, network delays, etc., where each component has a local physical environment that can be correlated with other local environments. To make the verification of such systems feasible, we have extended the PALS methodology to hybrid systems, and have given a bisimulation equivalence between the distributed model and the much simpler “synchronous” model, which abstracts from message exchange (and the resulting interleavings), network delays, execution times, etc. However, Hybrid PALS cannot abstract from imprecise local clocks and the timing of sensing and actuating.

We have shown that verification problems for Hybrid PALS synchronous models (and, by our bisimulation result, the corresponding distributed hybrid systems) such as bounded reachability analysis, unbounded inductive reasoning, and compositional assume-guarantee reasoning, can be expressed as SMT formulas over the real numbers. We have verified safety properties of a number of non-trivial distributed hybrid systems, with nonlinear ODEs and continuous physical connections between different components, using dReal.

Future work should develop SMT techniques for finding inductive invariant and compositional I/O conditions for nonlinear distributed hybrid systems.

8. REFERENCES


