A Hybrid Programming Language for Formal Modeling and Verification of Hybrid Systems

Eduard Kamburjan
Department of Informatics, University of Oslo, Norway
Department of Computer Science, Technische Universität Darmstadt, Germany

Stefan Mitsch
Computer Science Department, Carnegie Mellon University, USA

Reiner Hähnle
Department of Computer Science, Technische Universität Darmstadt, Germany

Abstract
Designing and modeling complex cyber-physical systems (CPS) faces the double challenge of combined discrete-continuous dynamics and concurrent behavior. Existing formal modeling and verification languages for CPS expose the underlying proof search technology. They lack high-level structuring elements and are not efficiently executable. The ensuing modeling gap renders formal CPS models hard to understand and to validate. We propose a high-level programming-based approach to formal modeling and verification of hybrid systems as a hybrid extension of an Active Objects language. Well-structured hybrid active programs and requirements allow automatic, reachability-preserving translation into differential dynamic logic, a logic for hybrid (discrete-continuous) programs. Verification is achieved by discharging the resulting formulas with the theorem prover KeYmaera X. We demonstrate the usability of our approach with case studies.

2012 ACM Subject Classification Computing methodologies → Distributed programming languages; Computing methodologies → Model verification and validation; Theory of computation → Logic and verification; Theory of computation → Timed and hybrid models

Keywords and Phrases Active Objects, Differential Dynamic Logic, Hybrid Systems

Digital Object Identifier 10.4230/LITES.8.2.4


Funding This work is partially supported by the FormbaR project, part of AG Signalling/DB RailLab in the Innovation Alliance of Deutsche Bahn AG and TU Darmstadt. This material is based upon work supported by AFSOR grant FA9550-16-1-0288.

Received 2020-06-10 Accepted 2022-05-11 Published 2022-12-07

Editor Alessandro Abate, Uli Fahrenberg, and Martin Fränzle

Special Issue Special Issue on Distributed Hybrid Systems

1 Introduction

Networked cyber-physical systems (CPS) are a main driving force of innovation in computing, from manufacturing to everyday appliances. But to design and model such systems poses a double challenge: first, their hybrid nature, with both continuous physical dynamics and complex computations in discrete time steps. Second, their concurrent nature: distributed, active components (sensors, actuators, controllers) execute simultaneously and communicate asynchronously. It is notoriously difficult to get CPS models right. Formal modeling languages, including hybrid automata [5], hybrid process algebra [27], and logics for hybrid programs [65], can be used to formally verify properties of CPS. Contrary to simulation frameworks, such as Ptolemy [71] or Simulink, however, these languages were designed for verification and are based on concepts of the underlying verification technology: automata, algebras, formulas. Their minimalist
syntax lacks standard structuring elements of programming languages such as types, scopes, methods, complex commands, futures, etc. Thus it is hard to adequately represent concurrently executing, communicating, hybrid components with symbolic data structures and computations, for example, servers or cloud applications.

Moreover, “low-level” models are hard to validate, i.e. to ensure that a CPS model reflects the designer’s intention, because these formalisms are not (efficiently) executable. To bridge the modeling gap we propose a high-level programming-based approach to formal modeling and verification of hybrid systems.

The basis of our approach is an Active Objects (AO) language [29] called ABS [48]. AO languages combine OO programming with strong encapsulation as well as asynchronous, parallel execution. Their concurrency model permits to decompose concurrent execution into sequential execution in a compositional manner. We chose ABS for its formal semantics, its open source implementation tool chain, and its demonstrated scaling on massively distributed systems [75], but our approach is applicable to other AO languages. ABS is efficiently executable via compilation to ERLANG and was used to model complex, real-world systems for cloud processing [3], virtualized services [49], data processing [56], and railway operations [53]. However, it lacks the capability to model hybrid systems. The first main contribution of this paper is the design of the Hybrid ABS (HABS) language, a conservative (syntax and semantics preserving) extension of ABS, generalizing the Active Objects paradigm to Hybrid Active Objects (HAO): AO with continuous dynamics. Obviously, it is necessary to accordingly extend the formal semantics of ABS and its runtime environment. This is our second main contribution. Our third main contribution is the implementation of HABS and a formal verification tool for it.

Our approach to formal verification of HABS programs is based on reachability-preserving translation into an existing verification formalism for hybrid programs. We choose differential dynamic logic (dL) [66, 68, 69], as implemented in the KeYmaera X system [36], because it is based on an imperative programming language that is a good match for the sequential fragment of HABS and verification in dL has been demonstrated to scale to realistic systems (e.g., [47]). The translation from HABS to dL involves to decompose a given HABS verification problem into a set of independent sequential dL problems. This is possible, because we impose an interaction pattern for communication on HABS that is less restrictive than available component-based techniques [64], yet is general enough to permit intuitive and concise modeling of relevant case studies. The identification of this pattern, the generation of dL verification conditions, and a reachability preservation theorem constitute our fourth main contribution.

The overall approach is illustrated in Fig. 1: A CPS is modeled as an HABS program with the aim to analyze its properties statically. One formulates desired properties as invariants that are formally verified to hold under certain assumptions. Before verification is attempted, the model is validated by executing it in the runtime environment to ensure that it behaves as intended. A visualization component helps to analyze behavior over time. Subsequently, the verification claim is automatically decomposed and translated into a set of dL verification problems discharged in KeYmaera X (optionally, formally verified runtime monitors [63] and formally verified machine code is available from KeYmaera X through VeriPhy [18]). Both, unexpected runtime behavior and failed verification attempts, serve to fix the model and/or the claimed properties.

The paper is structured as follows. Sect. 2 gives an informal example of an HABS model with a distributed water tank controller. Sect. 3 formally defines syntax and semantics of HABS. Sect. 4 describes modeling patterns. Sect. 5 gives theoretical background on dL, the translation into dL, the decomposition theorem, and tells how to prove correctness. It also contains a distributed controller case study. Finally, Sect. 6 discusses related and future work and concludes.
2 Distributed Hybrid Systems by Example

Active Objects [29] are objects that realize actor-based concurrency [44] with futures [28] and cooperative scheduling: Active Objects communicate via asynchronous method calls. On the caller side, each method invocation generates a future as a handle to retrieve the call’s result, once it is available. The caller may synchronize on that future, i.e. suspend and wait until it is resolved. At most one process is running on an Active Object at any time. That process suspends when it encounters the synchronization statement `await` on an unresolved future or a false Boolean condition. Once the guard becomes true, the process may be re-scheduled. All fields are strictly object-private.

Running a Hybrid Active Objects (HAO) model of a CPS can be pictured as follows: each object is capable of modeling a physical object, for example, a water tank. It may declare physical behavior via ordinary differential equations (ODEs) over “physical” fields, as well as discrete behavior via class and method declarations that can be used to control physical behavior. Once an HAO starts executing, the values of the physical fields evolve, governed by their ODEs, even when the controller is idle. This models the intuition that a physical system evolves independently of any observers and controllers.

Object orientation allows natural modeling of hybrid systems: continuous behavior is attached to an object, not a process. Processes realize discrete control behavior related to sensors and controllers. Specifically, the controller methods of an object may wait to execute until a certain physical state is reached (event-triggered control, for example, “tank is nearly full”). This “sensing” is modeled with getter methods of physical fields. Obviously, for validation the HABS runtime system must solve the differential equations in the physical model to determine the time point when such a waiting controller can start at the earliest; for verification, ODEs need not be solvable; they are analyzed with invariant-based techniques [67, 70]. Another communication pattern for controllers – time-triggered control – is provided by fixed sampling durations. More complex control patterns can be realized by waiting until the result of a subcomputation, i.e. a future, is ready.

Whenever a control process is activated, it can modify the physical state through actuators (for example, close a valve). In consequence, there are no timed race conditions, but the physical state might be changed by any process at the time it is scheduled. Actuation is modeled with setter methods of physical fields. Execution of control methods is assumed to take no physical time, unless explicitly modeled to do so.

Generally, a CPS can be modeled by several HAOs that communicate with each other via asynchronous method calls, for example, modeling a central controller. Often a controller object has no associated physical behavior; vice versa, an object that models physics, may not contain any control, but only sensor and actuator methods.

We demonstrate HAOs using three variants of water tank models. The first model, `TankMono`, is a single water tank that keeps its water level between two thresholds. It is modeled as a single object that integrates control and physics. The second model, `TankTick`, is also a single water tank,
but it is modeled with two separate objects for tank and controller. The final model, TankMulti, is a distributed system of \( n \) TankMono tanks that, in addition to the local threshold, maintain a global threshold over the sum of all local water levels.

2.1 Base System: TankMono

```java
interface ISingleTank {
    /* ensures 3 <= outLevel() <= 10 */
    Real outLevel();
    /* ensures -1/2 <= outDrain() <= 1/2 */
    Real outDrain();
    /* requires 4 <= inVal <= 9 */
    class CSingleTank(Real inVal) implements ISingleTank {
        /* invariant
           3 <= level <= 10 & -1/2 <= drain <= 1/2 & (drain<0->level>3) & (drain>0->level<10) */
        physical {
            Real level = inVal : level' = drain;
            Real drain = -1/2 : drain' = 0;
            Unit run() { this.ctrl(); }
            Unit ctrl() {
                await diff (level<=3 & drain<=0) | (level>=10 & drain>=0);
                if (level <= 3) drain = 1/2;
                else drain = -1/2;
                this.ctrl();
            }
            Real outDrain() { return this.drain; }
            Real outLevel() { return this.level; }
        }
    }
}
```

**Figure 2** TankMono: A water tank as a single HAO.

Fig. 2 shows an HAO model of a water tank whose physical section makes it either fill with \( \frac{11}{12} \text{l/sec} \) or drain at the same rate, according to the initial values and governing ODEs of the level and drain fields. Method ctrl() realizes a control loop that switches the drain field between those states so that the water level stays between 3l and 10l. The controller ctrl waits until the water level reaches the upper or lower limit, i.e. until the condition in Fig. 2, Line 21 holds. Depending on the case, it changes the state and calls itself recursively.

The JML style [20] comments in Fig. 2 contain an assumption on the initial state of inVal and a conjectured safety invariant and conjectured output guarantees that, in this case, can be proven: if the initial level is between 4l and 9l, then it always stays between 3l and 10l. Note that Lines 13–14 express a safety invariant that must be shown to be true, rather than control conditions. Intuitively, Line 13 expresses the property that the tank won’t drain below a threshold (level > 3) even if water is leaking from it (drain < 0). Similarly, Line 14 expresses that the tank won’t overflow (level < 10) even if water is pumped into the tank (drain > 0). Prior to formal verification of this property one typically runs tests to see whether the model behaves as intended. Our implementation allows to simulate and visualize an HAO model. The graph in Fig. 3 shows the behavior of a CSingleTank object instantiated with inVal = 5. In Sect. 5 we show how the class is translated into dL and how to prove the safety invariant in KeYmaera X for any object created with a parameter that satisfies the precondition. The only methods exposed to clients in the interface are outDrain() and outLevel().

2.2 Discrete Controller: TankTick

The ctrl() method in TankMono corresponds to a perfect sensor/controller that physically reacts to the water level and drain. TankTick splits controller and sensor into two objects and uses a clock to read the water level at certain intervals. This corresponds to a closed-loop control system with a discrete-time controller that samples the plant behavior.

Fig. 4 shows a water tank realized by a controller FlowCtrl and a Tank implementation CTank. The tank has an in-port (setter) method inDrain() and an out-port (getter) method outLevel(). It has no active discrete behavior on its own (the run method is empty), but its state changes nonetheless due to the continuous physical block. The FlowCtrl controller’s fields drain, level are
interface Tank {
  requires −1/2 <= newD <= 1/2;
  ensures 3 <= outLevel() <= 10;
  outLevel();
}

class CTank(Real inVal) implements Tank {
  physical {
    Real level = inVal; level' = drain;
    Real drain = -1/2; drain' = 0;
  }
  Unit run() {
  }
  Unit ctrlFlow() {
    await duration(tick,tick);
    level = t.outLevel();
    if (level <= 3.5) drain = 1/2;
    if (level >= 9.5) drain = -1/2;
    t!inDrain(drain);
    this.ctrlFlow();
  }
}

class FlowCtrl(Tank t, Real tick, Real inVal) {
  invariant (drain > 0 => level <= 9.5)
  & (drain < 0 => level >= 3.5)
  requires 0 < tick < 1 & inVal > 3.5
  Unit run() {
  }
  Unit ctrlFlow() {
    await duration(tick,tick);
    level = t.outLevel();
    if (level <= 3.5) drain = 1/2;
    if (level >= 9.5) drain = -1/2;
    t!inDrain(drain);
    this.ctrlFlow();
  }
}

interface Tank {
  inDrain(Real newD);
  ensures 3 <= outLevel() <= 10;
}

class CTank(Real inVal) implements Tank {
  physical {
    Real level = inVal; level' = drain;
    Real drain = -1/2; drain' = 0;
  }
  Unit run() {
  }
}

2.3 Distributed Tank Control: TankMulti

Consider a system where $n$ water tanks are monitored by a central controller that aims to keep the sum of all water levels between some thresholds. The code in Fig. 6 shows a controller that monitors a list of ISingleTank (Fig. 2) instances. Each tick seconds the central controller iterates over the list of tanks and if their combined level is almost at the upper threshold, the controller
drains all water tanks with rising levels (analogously for the lower threshold). Single water tanks still ensure that their local thresholds are observed. To allow the CControl instance to manipulate the ISingleTank instances, we add the following method to CSingleTank (and an analogous method to the interface):

```java
1 1/* requires newD > 0 */
2 2/* requires newD < 0 */
3 3/* requires -1/2 <= newD <= 1/2 */
4 Unit inDrain(Real newD) { this.drain = newD; }
```

Contrary to the contract in TankTick, we do not need to specify how frequently the method is called, because this information is available in the guard of the ctrl method of the instances. The recursive call at the end of ctrl ensures that there is always one process executing ctrl for each instance of FlowCtrl.

The graph in Fig.6 shows the simulation output for four water tanks with different initial values. The upper thresholds are managed by the distributed controller and the water tanks cooperatively: Only tanks 1 and 4 reach their local upper thresholds, the others are drained by the distributed controller to maintain the global threshold. The lower local thresholds are managed locally, the lower global threshold is never reached.

### 2.4 Futures

Future-based communication allows to decouple the call of a method from retrieving its result. For example, consider the code in Fig. 7. Class Node can perform some complex and time consuming computations on behalf of class Client. To enable load balancing the client has only a reference to an interface Server, which relays its request. The Server performs basic load balancing by a round-robin scheduling on a list of nodes. It then returns to the issuing client the future of the relayed request without having to wait for the computation to finish (Line 17). The client can then retrieve the future (Line 7) to synchronize on it without blocking the interface server (Line 8).

### 3 Hybrid Active Objects

An informal description of the intended semantics of Hybrid Abstract Objects in the Hybrid Abstract Behavioral Specification (HABS) language was provided in Section 2. The present section gives a formal account of its syntax and semantics. HABS is an extension of the Active Object language ABS [48]. ABS itself extends standard OO concepts as follows:

Encapsulation. All fields are strictly object-private.
```java
class CControl(List<ISingleTank> tanks,
    Real totalLower,
    Real totalHigher,
    Real tick)
  implements IControl {
    Unit run() {
      await duration(tick, tick);
      Real total = 0;
      List<ISingleTank> lower = list[];
      List<ISingleTank> higher = list[];
      foreach (next in tanks) {
        Real val = next.outLevel();
        Real dir = next.outDrain();
        if (dir < 0 && val > 3) lower = Cons(next, lower);
        if (dir > 0 && val < 10) higher = Cons(next, higher);
        total = total + val;
      }
      if (total <= totalLower+1)
        foreach (lnext in lower ) lnext!inDrain(1/2);
      if (total >= totalHigher-1)
        foreach (hnext in higher ) hnext!inDrain(-1/2);
      this.run();
    }
  }
```

**Figure 6** TankMulti: A controller for *n* TankMono instances and an example simulation output. Interface omitted.

**Cooperative Scheduling.** Active Objects cannot be preempted: a process running in an object may not be interrupted by other processes, unless the active process suspends itself or terminates.

**Asynchronous Calls, Futures.** All method calls to other objects are asynchronous. Every call not only generates a process on the callee side, but a future that points to that process. A process may pass around a future or synchronize with it to read the return value of the associated process once it has terminated.

As a **Timed Active Object language**, HABS also features:

**Simulation Time.** HABS allows to manipulate *simulation time* by explicitly advancing (and reading) an internal clock with specific statements. Simulation time is independent of the wall time.

### 3.1 Syntax

The syntax of HABS is given by the grammar in Fig. 8 and explained in the following section. With e we denote standard expressions over fields f, variables v and operators |, &, >=, <=, +, -, *, /.

Types T are all interface names, type-generic futures Fut<T>, lists List<T>, Real, Int, Unit and Bool. We also assume the usual functions for lists, etc.

A program contains a main method Main, interfaces ID and classes CD. Interfaces are standard, the main method contains a list of object creations. Classes can have parameters Tf, these are fields being initialized during object creation. Classes have fields FD, methods Met, an optional run method Run to start a process, and an optional physical block Phys that declares physical fields. A declaration of a physical field is a field declaration followed by a differential equation.

A differential equation is an equation between two differential expressions, which are standard expressions extended with a derivation operator e' for ddt. HABS supports explicit autonomous differential equations. The differential expressions and the field initialization form an initialized ordinary differential equation, e.g., Real f = 0: f' = 5-f. Note that f = 0 specifies the initial value of f, whereas the differential equation f' = 5-f is phrased in terms of the time-varying value of f, so models logarithmic growth towards f = 5.
class Node {
    Real compute_internal(Real r1, Real r2, Real r3) {... }
}
class Client(Server s) {
    Unit run() {
        Fut<Real> ffr = s!compute(1,2);
        Fut<Real> fr = ffr.get;
        Real r = fr.get;
        ...
    }
}
class Server(Queue<Node> internal, Real param) {
    Fut<Real> compute(Real r1, Real r2) {
        Node n = internal.pop();
        Fut<Real> fr = n!compute_internal(r1, r2, param);
        internal.push(n);
        return fr;
    }
}

Figure 7 An example for load balancing using futures. Interfaces omitted.

Figure 8 HABS grammar. T ranges over types, I over interfaces and C over classes. Differential expression \( e' \) are normal expressions extended with a derivation operator \( e' \).

Methods and statements are mostly standard, we focus on HAO-specific constructs. Methods are called asynchronously with \( e!m(e) \), i.e., after the call, the caller continues execution without waiting for the callee to finish. Instead, the caller generates a future. A future identifies the call and can be passed around by the caller. A process interacts in two ways with a future: either by awaiting its result with \( \text{await } e? \) on the guard \( e? \), or by reading its value with \( e.get \). Statements \( e.get \) block the reading object – no other process may run on it. In contrast, statements \( \text{await } g \) release the process control over the object while waiting for the guard \( g \) to hold. The guard is either a future guard \( e? \), a differential guard \( \text{diff } e \), or a timed guard \( \text{duration } (e1,e2) \). The future guard \( e? \) awaits the result of future \( e \), the differential guard \( \text{diff } e \) suspends the process until the

Program ::= ID CD Main  ID ::= interface I [extends I]?)?{MS} Programs, Interfaces
Main ::= {s?} Main
CD ::= class C [implements I]?)?[\{F D Met Run\}]? Classes
Run ::= Unit run() [s] FD ::= T f = e Run Method and Fields
Phys ::= physical \{DED\} DED ::= Real f = e : f' = e Physical Block
MS ::= T m(T) Met ::= MS \{s;return e;\} Signatures, Methods
s ::= while (e) \{s\} | if (e) \{s\} else \{s\}? | s; s Statements
| await g | [T? e]? = rhs Guards
\quad g ::= duration(e,e) | diff e | e?
rhs ::= e | new C(e) | e.get | em(e?) RHS Expressions
expression $e$ evaluates to true, and the timed guard $\text{duration}(e_1, e_2)$ suspends the process for at least $e_1$ time units$^1$. The notation $T v = o.m()$ is short for $\text{Fut}\langle T \rangle f = o!m(); T v = f$.get; (a call followed by a synchronization).

### 3.2 Semantics of HABS

HABS extends the structural operational semantics (SOS) for Timed ABS [16] in three aspects:

(i) it includes physical behavior in the object state;

(ii) determines whether a differential guard holds and, if not, when it will at the earliest;

(iii) updates the state whenever time passes.

This affects only expression evaluation and auxiliary functions. No new SOS rule is needed. In the following we extend the core of the ABS SOS semantics [16] to hybrid systems.

#### 3.2.1 States

The state of an object has three parts:

(i) a store $\rho$ that maps (physical and non-physical) fields to values, and the variables of the active process$^2$ to values;

(ii) $\text{ODE}$, the differential equations from its physical block;

(iii) $F$, the set of current solutions of $\text{ODE}$$^3$.

A solution $f$ is a function from time to a store which only contains the physical fields. The set $F$ may change, because the ODEs are solved as an initial-value problem with the current state of the physical fields as the initial values. For each $f \in F$ and each physical field $f$ the following holds: $f(0)(f) = \rho(f)$, i.e., the initial value $f(0)(f)$ of physical field $f$ is the current value $\rho(f)$ in the store $\rho$. We denote the solutions of $\text{ODE}$ with initial values from $\rho$ by $\text{sol}(\text{ODE}, \rho)$. We define runtime configurations formally:

$$
tcn ::= \text{clock}(e) \quad cn ::= cn \mid fn \mid msg \mid ob
$$

$$
ob ::= (o, \rho, \text{ODE}, F, \text{prc}, \text{prc}) \quad msg ::= \text{msg}(o, \bar{e}, f)
$$

$$
\text{prc} ::= (\tau, f, rs) \mid \bot \quad rs ::= s \mid \text{suspend}; s \quad \text{fat} ::= \text{fut}(f, e)
$$

**Figure 9** Runtime Syntax of HABS.

- **Definition 1** (Runtime Configuration [16]). The runtime syntax of HABS is summarized in Fig. 9: $f$ ranges over future identities, $o$ over object identities, $\rho, \tau$ over stores, i.e., assignments from fields or variables to values. A timed configuration has a clock $\text{clock}(e)$ with the current time, as an expression of $\text{Real}$ type and an object configuration $cn$. An object configuration $cn$ consists of messages $msg$, futures $\text{fat}$, objects $ob$, and can be composed $cn \mid cn$ (as usual, composition is commutative and associative). A message $\text{msg}(o, \bar{e}, f)$ records callee $o$, passed parameters $\bar{e}$ and the generated future $f$. A future configuration $\text{fut}(f, e)$ connects the future $f$ with its return value $e$. An object $(o, \rho, F, \text{ODE}, \text{prc}, \text{prc})$ has an identifier $o$, an object store $\rho$, the current solutions $F$, an active process $\text{prc}$ and a queue of inactive processes. $\text{ODE}$ is taken from the class declaration.

---

1. The parameter $e_2$ is used by certain scheduling policies [16], and is not relevant for HABS.
2. Recall that the active process executes the ABS methods, it does not relate to physical behavior.
3. The solutions computed relative to the initial values (state) at the last suspension.
A process is either terminated $\perp$ or has the form $(\tau,f,rs)$: the process store $\tau$ with current state of the local variables, its future $f$, and the statement $rs$ left to execute. The runtime syntax also allows the `suspend` statement, which is used to deschedule a process. Dotted underlined elements are an extension of HABS relative to ABS (also in Fig. 10 below).

Given a process store $\tau$ and an object store $\rho$ we use $\sigma = \rho \circ \tau$ to denote the state of both fields and local variables. We first define the evaluation of expressions and guards.

### 3.2.2 Evaluation of Expressions

Expressions $e$ are evaluated with a function $J_{e}^{F,t}$ over a store $\sigma$ and a set of solutions $F$ at $t$ time units in the future. The semantics of expressions containing physical fields is as follows.

**Definition 2 (Semantics of Expressions).** Let $F$ be the set of solutions. Given a store $\sigma$, we can check whether $F$ is a model of an expression $e$ after $t$ time units. Let $f_p$ be a physical field and $f_d$ a non-physical field of $o$. The semantics of fields $f_p$, $f_d$, unary operators $\sim \in \{!,\neg\}$ and binary operators $\oplus \in \{|,\&,\geq,\leq,+,–,*,/\}$ is defined as follows:

- $[f_d]_{\sigma}^{F,t} = \sigma(f_d)$
- $[f_p]_{\sigma}^{F,t} = \begin{cases} v & \text{if } \forall f \in F. v = f(t)(f_p) \\ \infty & \text{otherwise} \end{cases}$
- $[\sim e]_{\sigma}^{F,t} = \sim[e]_{\sigma}^{F,t}$
- $[e_1 \oplus e_2]_{\sigma}^{F,t} = [e_1]_{\sigma}^{F,t} \oplus [e_2]_{\sigma}^{F,t}$

Outside differential guards, only the evaluation in the current state $[e]_{\sigma}^{F,0}$ is needed, which is $\rho(f_p)$ from $f(0)(f_p)$ and this expression is never $\infty$. We identify $[e]_{\sigma}^{F,0}$ and $[e]_{\sigma}$ with $[e]_{\sigma}^{F,0}$.

### 3.2.3 Evaluation of Guards

The semantics of an `await g` statement is to suspend until the guard holds, i.e. until $[g]_{\sigma}^{F}$ evaluates to true. For example, a duration guard $\text{duration}(e_1,e_2)$ evaluates to true if $[e_1]_{\sigma}^{F} \leq 0$. Defining the semantics of guards requires two operations: An extension of the evaluation function that returns true if the guard holds and the maximal time elapse $\text{mte}_{\sigma}$ returning the time $t$ that may elapse before the guard evaluates to true, or $\infty$ if it never does.

First we define $\text{mte}(e)$: the maximal time that may elapse without missing an event is the minimal time needed by the system to evolve into a state where the guard is guaranteed to hold. This yields also the semantics of the guard itself.

**Definition 3 (Semantics of Differential Guards).** Let $F$ be the set of solutions of object $o$ in state $\sigma$. Then we define:

$$\text{mte}_{\sigma}^{F}(\text{diff } e) = \arg\min_{t \geq 0} \left( [e]_{\sigma}^{F,t} = \text{true} \right)$$

$\text{diff } e$ is evaluated to true if no time advance is needed:

$$[\text{diff } e]_{\sigma}^{F,0} = \text{true} \iff \text{mte}_{\sigma}^{F}(\text{diff } e) = 0$$

If $e$ contains no continuous variable then the differential guard semantics and the evaluation of expressions in Def. 2 coincides with condition synchronization and expression evaluation in the standard ABS semantics [48].
We follow the original ABS semantics, where suspension is handled with a separate \texttt{suspend} statement for reasons of uniformity – in principle, rules (1)+(2) could be combined.

\section*{3.2.4 Transition System}

Fig. 10 gives the most important rules for the semantics of a single object, the omitted rules are given in [16]. Rules (1)–(3) define the semantics of process suspension. An \texttt{await} statement suspends the current process and gives other processes in the queue \(q\) a chance to run, even if its guard is evaluated to true. Suspension is modeled in rule (1) simply by introducing a \texttt{suspend} statement in front of the \texttt{await}.\footnote{We follow the original ABS semantics, where suspension is handled with a separate \texttt{suspend} statement for reasons of uniformity – in principle, rules (1)+(2) could be combined.} Rule (2) realizes a \texttt{suspend} statement by moving the current process to the object’s queue. As explained in Sect. 3.2.3, upon reactivation of a suspended process we must ensure its guard to be true, relative to the solution of \texttt{ODE} with \emph{initial values at suspension time}. Therefore, rule (2) also recomputes the solutions \(F\). Rule (3) can then re-activate a process beginning with an \texttt{await} statement, simply by checking whether its guard evaluates to true at current time (advancing time in timed configuration is explained below). An analogous rule (not shown in Fig. 10) activates a process with any other non-\texttt{await} statement. Rule (4) evaluates an assignment to a local variable. The rule for fields is analogous. Rule (5) realizes a termination (with solutions of the ODEs) and (6) a future read. Finally, (7) is a method call, the rule for transforming a message into a process is straightforward.

For configurations, there are two rules, shown in Fig. 11. Rule (i) realizes a step of some object without advancing time, only if \(p\) is not applicable, i.e. all ABS processes are blocked, rule (a) can be applied. It computes the global maximal time elapse \(mte\) and advances the time in the clock and all objects. In particular, it decreases syntactically the timed guards.

\begin{itemize}
\item [(i)] \(\text{clock}(t)\ cn\ cn_1 \rightarrow \text{clock}(t)\ cn_2\ cn_1\) with \(cn \rightarrow cn_2\)
\item [(a)] \(\text{clock}(t)\ cn \rightarrow \text{clock}(t+\tilde{t})\ \text{adv}(cn,\tilde{t})\) if (i) is not applicable and \(mte(cn) = \tilde{t} \neq \infty\)
\end{itemize}
Fig. 12 shows the auxiliary functions and includes the full definition of $mte$. Note that $mte$ is not applied to the currently active process, because, when (1) is not applicable, it is currently blocking and, thus, cannot advance time. The characteristic feature of hybrid objects is that their physical state changes when time advances, even when no process is active. This is expressed in the semantics by a function $adv(\sigma, t)$ which takes a state $\sigma$, a duration $t$, and advances $\sigma$ by $t$ time units. For non-hybrid Active Objects $adv(\sigma, t) = \sigma$. There, the function is needed only to modify the process pool of an object for scheduling, not its state, and is used exactly as in [16].

\[
mte(cn_1, cn_2) = \min(mte(cn_1), mte(cn_2)) \quad mte(\text{msg}) = mte(\text{fut}) = \infty
\]

\[
mte(o, \rho, \text{ODE}, F, \text{proc}, q) = \lfloor \min(mte(q), \infty) \rfloor_{\rho} \quad mte(\tau, f, \text{await } g; s) = [mte(g)]_{\tau}
\]

\[
mte(\tau, f, s) = \infty \text{ if } s \neq \text{await } g; \bar{s} \quad mte(\text{duration}(e_1, e_2)) = e_1
\]

\[
mte_\sigma(\text{diff } e) = \text{argmin}_{t \geq 0} \left( [e]_t = \text{true} \right) \quad mte(\text{e?}) = \infty
\]

\[
adv(cn_1, cn_2, t) = adv(cn_1, t) \quad adv(cn_2, t)
\]

\[
adv(\text{msg}, F, t) = \text{msg} \quad adv(\text{fut}, F, t) = \text{fut}
\]

\[
adv(o, \rho, \text{ODE}, F, \text{proc}, q), F, t) = (o, adv(\rho, t), \text{ODE}, F, adv(\text{proc}, F, t), adv(q, F, t))
\]

\[
adv(\bot, F, t) = \bot
\]

\[
adv(\tau, f, s), F, t) = (\tau, f, s) \text{ if } s \neq \text{await duration}(e_1, e_2); \bar{s}
\]

\[
adv(\tau, f, \text{await duration}(e_1, e_2); s), F, t) = (\tau, f, \text{await duration}(e_1 + t, e_2 + t); s)
\]

\[
adv(\sigma, t)(\bar{t}) = \begin{cases} 
\sigma(t) & \text{if } f \text{ is not physical} \\
v & \text{if } \forall f \in F. v = f(t)(\bar{t})
\end{cases}
\]

![Figure 12](image.png)

Figure 12 Auxiliary functions. Lifting to lists is not shown.

The $adv$ auxiliary function handles uniqueness w.r.t. the solutions of the ODE at the points in time where the solutions are accessed: Note that the solutions are handled as a set $F$: at time $t$ function $adv$ checks that all solutions coincide at this point in time. If this is not the case, or if no solution can be found by the implementation, a runtime error is thrown. Also, all solutions are computed without restrictions on the time domain (e.g., for how long they exit) because it is not known for how long the dynamics are followed at this point. Alternatively, one could either impose restrictions on the ODE to enforce uniqueness or non-deterministically choose one of the solutions.

We can now define traces of programs and objects.

**Definition 4 (Traces).** Given a program $\text{Prgm}$, we denote with $\text{clock}(0)$ $cn_0$ the initial state configuration [16]. A run of $\text{Prgm}$ is a (possibly infinite) reduction sequence

\[
\text{clock}(0) \rightarrow cn_0 \rightarrow \text{clock}(t_1) \rightarrow cn_1 \rightarrow \cdots
\]

The trace $\theta_o$ of an object $o$ in a run is an assignment from the dense time domain $\mathbb{R}^+$ to states. We say that $\text{clock}(t_i) \rightarrow cn_i$ is the final configuration at $t_i$ in a run, if any other timed configuration $\text{clock}(t_i) \rightarrow cn_i$ is before it. Fig. 13 gives a formal definition.

For any point in time $x$, the state of $o$ is taken from the run, if a reduction step was made at $x$ and $o$ was already created. The third case in the definition is illustrated in Fig. 14: At time points $y$ and $z$, discrete steps are done, but none at $x$. The state $\theta_o(x)$ is extrapolated from the state $\theta_o(y)$ by following solutions from the last step at point $y$, if $o$ is created.
\[ \theta_o(x) = \begin{cases} 
\text{undefined} & \text{if } o \text{ is not created yet} \\
\rho & \text{if } \text{clock}(x) \text{ is the final configuration at } x \\
\text{adv}(\rho, F, x - y) & \text{if there is no configuration at } \text{clock}(x) \\
& \quad \text{and the last configuration was at } \text{clock}(y) \\
& \quad \text{with state } \rho \text{ and solutions } F
\end{cases} \]

**Figure 13** Extraction of a trace \( \theta_o \) for an object \( o \) from a given run.

**Figure 14** Illustration of the state at time \( x \) and two discrete states with \( \text{clock}(y) \) and \( \text{clock}(z) \).

### 3.3 The Component Fragment

We define a sublanguage of HABS called Component HABS (CHABS) to model component-style architectures with in- and out-ports, as well as dedicated controllers with a read-evaluate-write cycle. Syntactically, a class is a component if it can be derived from the syntax in Fig. 8 with the rule for \( \text{Met} \) replaced by the following:

\[
\begin{align*}
\text{Met} &::= \text{MS} \mid \text{IPort} \mid \text{Ctrl} \\
\text{OPort} &::= \{ \text{return } \text{this}.f; \} \\
\text{IPort} &::= \{ \text{this}.f = v; \text{ return } \text{Unit}; \} \\
\text{Ctrl} &::= \{ \text{sa; si; sc; so; this.m();} \} \\
\text{sa} &::= \text{await duration}(e,e) | \text{await diff } e \\
\text{si} &::= \text{this}.f = e.m() | \text{si;si} \\
\text{sc} &::= \text{while } (e) \{ \text{sc} \} | \text{if } (e) \{ \text{sc} \} \text{ [else } \{ \text{sc} \}]? | \text{ sc;sc } | \text{T? e = e } | \text{ e!m(R)} \\
\text{so} &::= e!e.m(\text{this.f}) | \text{ so; so}
\end{align*}
\]

Additionally, we demand that the only numerical data types used are \( \text{Int}, \text{Real} \). Out-ports return the value of a field and in-ports copy a method parameter into a field. A controller method \( \text{Ctrl} \) has a timed or differential guard \( \text{sa} \), followed by reads \( \text{si} \) from the out-port methods of other objects (recall that \( \text{this}.f = e.m() \) is a shortcut for an asynchronous call followed by a read, not a synchronous call), computations \( \text{sc} \), and writes \( \text{so} \) to the in-ports of other objects. In the component fragment, we realize a component-based controller with a read-compute-write loop by restricting the \( \text{run} \) method of Fig. 8 to start a controller with an asynchronous call to an object’s own controller method \( \text{Ctrl} \) and each controller ends with a recursive call to itself. The TankMono and TankTick models are CHABS models, the central controller in TankMulti is not. A controller method with a differential guard is an event-triggered controller, a controller with a timed guard a time-triggered controller.

We model instantaneous controllers in CHABS: once controller is scheduled (i.e., after its guards evaluates to true) no time can pass because all calls in \( \text{Ctrl} \) are to port methods that cannot block the caller and neither suspensions nor future reads are allowed.
3.4 Simulation

The implementation of HABS extends the ABS compiler [81] to compute solutions for differential guards, time elapse, and state advance. To compile differential guards correctly, it needs to compute \( mte^F_\sigma(\text{diff } a) \) (Def. 3).

The ODEs of a class cannot be changed at runtime and are, therefore, represented as a string in the class table. The simulator uses an external solver to solve initial value problems and minimize/maximize duration between events.

Solutions To compute solutions \( F \), the ODEs and the current state of the physical fields are passed to Maxima [61] as an initial value problem. The solution is an equation system or an error. In its default setting, the simulator neither supports non-unique solutions nor non-solvable ODEs. The simulator, however, has the infrastructure to use solvers other than Maxima. This allows us to handle non-linear ODEs: by prefixing the physical block with \([1]\), the modeler can select the solver ic1 (instead of the default desolve), which can handle non-linear systems.

Time elapse After solving the initial value problem, Maxima is invoked with a minimization problem: it minimizes the time \( t \) with the equation system representing \( F \) as the constraints (this corresponds to eager mode switching in a hybrid automaton). The result is then handled in the same way as a parameter to a timed guard by the runtime system. Once time has passed and the suspended process is reactivated, the physical fields are updated according to \( F \). This uses the Maxima function fmin_cobyla.

State advance To implement the advance function \( adv \), if the state of the object changes any physical field, the procedure used to compute time elapse is repeated for every currently suspended differential guard to accumulate the result.

The output files used to visualize a program execution are of the form \( t_1, F_1, t_2, F_2, \ldots, F_n, t_n \). Here \( t_i \) are the points in time where the object schedules a process and \( F_i \) the function describing its physical behavior in the previous suspended state. Each time a differential guard is reactivated, not only its state is updated, but the solution \( F_{i+1} \) and the reactivation time \( t_{i+1} \) are written to the output. Each object has its own output file.

A Python script translates output files into a discrete dynamic graph in Maxima format which in turn calls gnuplot that is responsible for creating the graph. The graphs in this work are slightly beautified outputs.

4 Modeling with HABS

We give more examples of HABS models and discuss some design decisions in the language, as well as modeling patterns in HABS for common phenomena in hybrid system control.

4.1 Non-Linear Dynamics

HABS can handle non-linear ODEs and non-linear dynamics to the extent the backends support it. For an example, consider a resistor attached to an alternating current source that produces a sine-formed current. This is described by the class in Fig 15.

We use the non-linear solver of Maxima (by annotating \([1]\)). This solver requires the input to satisfy certain syntax constraints, which entail the slightly awkward specification \( r' = 0*t \). We must give an explicit ODE for each non-constant variable for KeYmaera X and as HABS requires an autonomous system, we add a clock variable time to express sine and cosine.

The example has a run method that illustrates validation. We check whether our simple model is in fact a resistor and adheres to the law \( R = I/V \): Even before visualization, we can use simple command line output to check \( I/V \) by sampling every 1 second. The output for an instance
class Resistor(Real init) {
  [1] physical {
  /* format expected by Maxima */
  Real t = 0: t’ = 1;
  Real r = init: r’ = 0*t;
  Real i = 0: i’ = cos(t);
  Real v = 0: v’ = r*cos(t);
  }
  Unit run() {
    await duration(1,1);
    println("step: " + toString(now()) + " with " + toString(v/i));
    if (timeValue(now()) < 60) this!run();
  }
}

Figure 15 A resistor attached to an AC-circuit and its sine-formed current.

Resistor(5) is shown in Fig. 15, where Time(n) is the symbolic time at the point of time when now() is evaluated. In the example this corresponds to seconds. As a next step, we can use the visualization to observe longer trends in Fig. 16, again for a Resistor(5).

Figure 16 Example simulation output of a Resistor(5).

Finally, we can formally verify the behavior with our translation approach to KeYmaera X by removing the run method and, thus, transforming it into a CHABS component.

4.2 Delays and Imprecision

Communication is imperfect in realistic models. We demonstrate how to model two such imperfections, delays and imprecision, in HABS. We use a simple platooning example, where a follower car wants to follow a lead car at a certain distance. Follower cars are modeled in the CHABS class FollowerCar in Fig. 17. For simplicity, the minimal (minDist) and maximal distance (maxDist) to the lead car are independent of the speed and the controller sampling frequency, which means the follower car will not provably stay in the desired distance interval. The time consuming statement await duration can be used to model two kinds of delays:

1. Complex computations that take some time to finish.
2. Latency: By adding a time consuming statement as the last statement of a method before the return, one can model delays in a network.
class FollowerCar
    (Real inita, Real start, 
     Real tick, Real minDist, 
     Real maxDist, ICar leadCar)
    implements ICar {
        Real next = start + minDist;
        physical {
            Real a = inita : a' = 0;
            Real v = 0 : v' = a;
            Real x = start : x' = v;
        }
        Unit run() {
            this!ctrlObserve();
        }
        Unit ctrlObserve() {
            await duration(tick, tick);
            next = leadCar.getPosition();
            if(next - x <= minDist) a = a/2;
            if(next - x >= maxDist) a = a*2;
            this.ctrlObserve();
        }
        Real getPosition() {
            return x;
        }
    }

Figure 17 Simple platooning example for a follower car following safely behind a lead car

For example, we extend getPosition() in FollowerCar to model sensing latency as follows:

    Real getPosition() {
        Real oldVal = x;
        await duration(1/10, 1/10);
        return oldVal;
    }

Like ABS, HABS has access to a (uniformly distributed) random number generator. There are 
functions to generate other statistical distributions. This allows to model imprecision/uncertainty. 
The following method adapts getPosition() to model sensor uncertainty:

    Real getPosition() {
        Real imp = (random(11) + 95)/100; // number between 0.95 and 1.05
        return this.level * imp;
    }

4.3 Variability Modeling

One of the main advantages of using a mature programming language as a host for hybrid behavior 
is that we can use its structuring elements and concepts: HABS inherits the module system with 
import/export clauses\(^5\), as well as the delta-oriented [73], feature-oriented [14] product line [8, 74] 
(DFPL) mechanisms of ABS [25] to model variability.

DFPLs define not a single model, but a set of models which are variants of each other. From a 
given core model, so-called code deltas define variants based on syntactic operations: removal, 
modification and addition of classes, methods and fields. A variant is obtained from the core 
model by applying modifications specified by the deltas to it.

To determine the relevant deltas, each delta has a set of features that activate its application. 
A feature of a variant corresponds roughly to one implemented feature of the modified model. A 
set of features is called a product. After selecting a product, the corresponding deltas are computed 
and applied, resulting in an HABS model without variability.

\(^5\) Omitted from the language syntax in Sec. 3 for brevity.
\textbf{delta} Delay;  
\textbf{modifies class} Cars.FollowerCar {  
\textbf{modifies} Real getPosition() {  
  Real old = \textit{original}();  
  \textbf{await duration}(1/10,1/10);  
  return old;  
  }  
}\textbf{delta} Imprecision;  
\textbf{modifies class} Cars.FollowerCar {  
\textbf{modifies} Real getPosition() {  
  return \textit{original}()*(\textit{random}(11)+95)/100;  
  }  
}\textbf{delta} CruiseControl;  
\textbf{modifies class} Cars.FollowerCar {  
\textbf{adds} Real ccTick = this.tick*2;  
\textbf{adds} Unit cruise() {  
  \textbf{await duration}(ccTick, ccTick);  
  if ((v >= 5 || v <= 0) && a != 0)  
  {  
    a = 0;  
  }  
  this.cruise();  
  }  
\textbf{modifies} Unit run() {  
  \textit{original}();  
  this!cruise();  
  }  
}\textbf{delta} CruiseControl \textbf{when} FCruiseControl; 
\textbf{delta} Delay \textbf{when} FDelay;  
\textbf{delta} Imprecision \textbf{after} Delay \textbf{when} FImprecision;  

ewcommand{\productline}{productline PL1;}  
\textbf{features} FDelay, FImprecision, FCruiseControl;  
\textbf{delta} CruiseControl \textbf{when} FCruiseControl;  
\textbf{delta} Delay \textbf{when} FDelay;  
\textbf{delta} Imprecision \textbf{after} Delay \textbf{when} FImprecision;  

\textbf{Figure 18} Product line based on Fig. 17 for variability in position readings and cruise control.  

We refrain from introducing the whole variability layer of \textit{ABS} and refer to [25] for a detailed and formal introduction. Instead, we use the platooning example in Fig. 17 to demonstrate variability modeling in practice. The changes for imprecision and delay, as well as adding a cruise control system can be modeled as a product line. This allows to select the appropriate car product for a concrete system, as summarized in Fig. 18. The product line consists of three deltas (Delay, Imprecision and CruiseControl), three features (FDelay, FImprecision and FCruiseControl) and a knowledge base that defines which features select which delta (\textbf{delta} D \textbf{when} F) and in which order deltas are applied if they modify the same method (\textbf{delta} D \textbf{after} D2).  

The \textbf{delta} Delay modifies class \textit{Cars.FollowerCar}\textsuperscript{6} and its method \texttt{getPosition()}. The modified method first calls the existing variant of the method via \textit{original} and then waits before returning the value. \textbf{Delta} Imprecision is similar. Both deltas modify the same method. There are numerous desirable properties, and to make the product line outcome deterministic, we must fix the order in which methods are applied that modify the same method. Here, we demand that Imprecision is applied after Delay. \textbf{Delta} CruiseControl adds a field and method implementing a simple cruise control system. Deltas may also remove methods and fields (not shown here). In our example we represent each delta as a feature, and so any product that refers to a feature invokes its assigned delta. The deltas are applied \textbf{syntactically} before type checking. As a result, a standard \textit{HABS} program is created. For example the product \{FDelay\} results in the code below.  

\begin{verbatim}
\textbf{class} FollowerCar (\ldots) \textbf{implements} ICar {  
  \ldots // as above  
  Real getPosition_core() { return x; }  
  Real getPosition() { \texttt{return this.getPosition_core()}*(\textit{random}(11) + 95)/100; }  
}\end{verbatim}

\footnote{\textit{Cars} is the module.}
5 Formal Verification of HABS Models

As a prerequisite for formal verification of HABS, we briefly review differential dynamic logic (dL) [68, 69] as implemented in the hybrid systems theorem prover KeYmaera X [36]. We then discuss translation from HABS to dL, and sketch formal verification in dL with sequent proofs.

5.1 Background: Differential Dynamic Logic

Differential dynamic logic expresses the combined discrete and continuous dynamics of hybrid systems in a sequential imperative programming language called hybrid programs. Its syntax and informal semantics are in Table 1.

<table>
<thead>
<tr>
<th>Program</th>
<th>Informal semantics</th>
</tr>
</thead>
<tbody>
<tr>
<td>?φ</td>
<td>Test whether formula φ is true, abort if false</td>
</tr>
<tr>
<td>x := θ</td>
<td>Assign value of term θ to variable x</td>
</tr>
<tr>
<td>x := ∗</td>
<td>Assign any (real) value to variable x</td>
</tr>
<tr>
<td>{x′ = θ &amp; H}</td>
<td>Evolve ODE system x′ = θ for any duration t ≥ 0</td>
</tr>
<tr>
<td></td>
<td>with evolution domain constraint H true throughout</td>
</tr>
<tr>
<td>α; β</td>
<td>Run α followed by β on resulting state(s)</td>
</tr>
<tr>
<td>α ∪ β</td>
<td>Run either α or β non-deterministically</td>
</tr>
<tr>
<td>α∗</td>
<td>Repeat α n times, for any n ∈ N</td>
</tr>
</tbody>
</table>

Hybrid programs provide the usual discrete statements: assignment (x := θ), non-deterministic assignment (x := ∗), test (?φ), non-deterministic choice (α ∪ β), sequential composition (α; β), and non-deterministic repetition (α∗). A typical modeling pattern combines non-deterministic assignment and test (e.g., “x := ∗; ?H”) to choose any value subject to a dL constraint H. Standard control structures are expressible, for example:

(i) if H then α else β ⊨ (?H; α) ∪ (?¬H; β),
(ii) if H then α ⊨ (?H; α) ∪ (?¬H),
(iii) while (H) α ⊨ (?H; α)∗; ?¬H.

For continuous dynamics, the notation {x′ = θ & H} represents an ODE system (derivative x′ in time) of the form x′ = θ₁, ..., x′ₙ = θₙ. Any behavior described by the ODE stays inside the evolution domain H, i.e. the ODE is followed for a non-deterministic, non-negative period of time, but stops before H becomes false. For example, a basic model of the water level in a tank draining with flow −f is given by the ODE {x′ = −f & x ≥ 0}, where the evolution domain constraint x ≥ 0 means the tank will not drain to negative water levels. With a careful modeling pattern, ODEs can be governed by H so that one can react to events, without restricting or influencing the continuous dynamics modeled in the ODE [72]: The pattern {x′ = θ & H} ∪ {x′ = θ & H} permits control intervention to achieve different behavior triggered by an event H. H is the weak complement of H: they share exactly their boundary from which both behaviors are possible. For example, H ⊨ x ≤ 0, H ⊨ x ≥ 0.

The dL-formulas φ, ψ relevant for this paper are propositional logic operators φ ∧ ψ, φ ∨ ψ, φ → ψ, ¬φ and comparison expressions θ ∼ η, where ∼ ∈ {<, ≤, =, ≠, ≥, >} and θ, η are real-valued terms over {+, −, ·, /}. In addition, there is the dL modal operator [α]φ. The dL-formula [α]φ is true iff φ holds in all states reachable by program α. The formal semantics of dL [68, 69] is a Kripke semantics in which the states of the Kripke model are the states of the hybrid system. The semantics of a hybrid program α is a relation [α] between its initial and final states. Specifically, ν ⊨ [α]φ iff ω ⊨ φ for all states (ν, ω) ∈ [α], so all runs of α from ν are safe relative to φ.
Proofs in $dL$ are sequent calculus proofs on the basis of $dL$ axioms. For example, validity of the $dL$ formula $x \geq 0 \rightarrow [x := x + 1 \cup x := 2; \{x' = 3\}]x \geq 1$ over a simple program that either increments the value of $x$ or continuously evolves $x$ with a constant slope $x' = 3$ after setting the initial value of the differential equation with $x := 2$ is shown in the sequent proof below:

Sequent proofs proceed bottom-up but validity transfers top-down, i.e., from the subgoals above the horizontal bar, the axiom or proof rule annotated to the left of the bar implies the sequent below the horizontal bar. In each step, assumptions are listed to the left of the →, and the alternatives to prove to the right of it. The proof starts with step →R to make the left-hand side $x \geq 0$ of the implication available as an assumption. Next, the non-deterministic choice step [; ] splits the sequential composition into nested box modalities, and then step [; ], hideL executes the assignment and weakens the now obsolete assumption $x \geq 1$, so with conjunction splitting $\land_R$ we get two subgoals: a left subgoal for the increment program $x := x + 1$ and a right subgoal for the differential equation program. On the increment program branch, we execute the assignment in step [:=] and the result follows by real arithmetic in step QE. On the differential equation branch, step [; ] splits the sequential composition into nested box modalities, and then step [; ], hideL executes the assignment and weakens the new obsolete assumption $x \geq 0$. The branch closes by differential induction dl (intuitively, the dl step expresses that $x \geq 1$ stays true along the flow of the differential equation, see [67]). This concludes the example proof.

5.2 Formal Verification of Components

```plaintext
interface Tank {
  // requires −1/2 <= newD <= 1/2; */
  Unit inDrain(Real newD); /* ensures 3 <= outLevel <= 10; */
  Real outLevel();
}

class CTank(Real inVal) {
  implements Tank {
    // requires newD > 0 -> level <= 9.5 */
    // requires newD < 0 -> level >= 3.5 */
    // timed._requires inDrain < 1 */
    Unit inDrain(Real newD) { ... }
  }
}

class FlowCtrl(Tank t, Real tick, Real inVal) {
  // invariant (drain > 0 -> level <= 9.5)
  // & {drain < 0 -> level >= 3.5} */
  ...
}
```

Figure 19 Annotations in the TankTick model, repeated from Fig. 4.

To establish system-wide properties, hybrid active objects must be shown to satisfy their class invariants, provided that the constraints expressed in the preconditions are met. We make this precise now. A class specification is a tuple $(\text{inv}, \text{pre}, \text{TReq}, \text{Req}, \text{Ens})$, where $\text{inv}$ is the class invariant
(annotated /* invariant ... */; see Fig. 19, lines 20–21), a dŁ formula over the fields and parameters of the class; pre is the precondition (annotated to class declarations with /* requires ... */; see Fig. 19, line 17), a dŁ formula over the initial values of fields and class parameters. TReq is the set of timed input requirements for in-port methods (annotated with /* timed requires ... */; see Fig. 19, line 12): dŁ formulas over a dedicated program variable with the method’s name. Req is the set of input requirements for in-port methods (annotated with /* requires ... */; see Fig. 19, lines 2, 10–11): dŁ formulas over fields and method parameters. Ens is the set of output guarantees for out-port methods (annotated with /* ensures ... */; see Fig. 19, line 4): dŁ formulas over a dedicated program variable with the method’s name.

To verify a class C against a class specification, both are translated into dŁ-formula (1) that expresses safety.

\[
\text{assumptions}_C \rightarrow [(\text{code}_C \oplus \text{plant}_C)^*] \text{safety}_C
\]  

The placeholders assumptions\(_C\), code\(_C\), plant\(_C\), and safety\(_C\) (defined formally in Sect. 5.3 below) encode class \(C\) and its specification (inv, pre, TReq, Req, Ens) as follows: The formula assumptions\(_C\) is the conjunction of pre and conditions on variables that keep track of time. As usual in controller verification, the program repeats a control part code\(_C\) followed by the continuous behavior plant\(_C\). The condition safety\(_C\) must hold after an arbitrary number of iterations. It combines inv with input requirements of in-port methods of referred objects and guarantees of own out-port methods.

Even though formula (1) safety\(_C\) is a postcondition that must hold only in the final states of the system, we stress that this means at every real time point during the continuous dynamics, because ODEs advance for a non-deterministic duration while discrete statements take no time. The modality, therefore, expresses that whenever code\(_C\) executes completely, the invariant holds. In particular, the invariant holds at the beginning of and throughout the evolution of the continuous dynamics in plant\(_C\). Thus, validity of formula (1) expresses safety of every correctly created object (with respect to its specification).

The following translation of an HABS class and its specification defines formally how the placeholders are composed. The translation is fully automatic and verification is compositional: only classes whose code changed explicitly need re-verification, not the whole system.

### 5.3 Translation from CHABS to dŁ

We use two operations on sets of programs \(P\). Operation \(\sum P\) constructs a program that non-deterministically executes one of the elements. Operation \(\prod P\) constructs all permutations of sequential element-wise execution. Let \(|P| = n:\n
\[
\sum P = \sum \{p_1, \ldots, p_n\} = p_1 \cup p_2 \cup \cdots \cup p_n \\
\prod P = \{p_1; \ldots; p_n \mid \forall i,j \leq n. \ p_i, p_j \in P \land (i \neq j \rightarrow p_i \neq p_j)\}
\]

We translate classes \(C\) with the following design restrictions:

1. All controllers update their local caches of other objects before providing information to those objects (for example, read the current water level before instructing the tank to drain or fill); local caches, once updated, are not modified later.
2. In-port methods with a timed input requirement are only called from timed controllers (for example, a tank that expects to be filled every 5 s is governed by a controller running at a corresponding frequency).
3. Duration statements are exact (have two identical parameters).
4. Local variable names are unique.
The formula
\[
\text{Trans}(f) \equiv f, \text{ where } f \text{ is a } dC \text{ variable representing field } f
\]
\[
\text{Trans}(v) \equiv v, \text{ where } v \text{ is a } dC \text{ variable representing variable } v
\]
\[
\text{Trans}(e_1 \text{ op } e_2) \equiv \text{Trans}(e_1) \text{ op } \text{Trans}(e_2)
\]
\[
\text{Trans}([T] v = e) \equiv \text{Trans}(v) := \text{Trans}(e)
\]
\[
\text{Trans}(\text{if}(e)[s] \text{ else } [s]) \equiv \text{if } (\text{Trans}(e)) \text{ then } \text{Trans}(s) \text{ else } \text{Trans}([s])
\]
\[
\text{Trans}(\text{while}(e)[s]) \equiv \text{while}(\text{Trans}(e)) \text{Trans}(s) \text{ where } \text{Trans}([s_1]; [s_2]) = \text{Trans}(s_1); \text{Trans}(s_2)
\]
\[
\text{Trans}(e = m()) \equiv \text{Trans}(e = e.m()) \equiv \text{Trans}(f) := \text{?}\text{?}_{\text{m}}
\]
where \(\varphi_{\text{m}}\) is the postcondition of \(m\), with the method name replaced by \(\text{Trans}(f)\).

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure20.png}
\caption{Translation of expressions \(e\) and statements \(s\).}
\end{figure}

The first two constraints fix the interaction pattern between components, the last two simplify the presentation. For classes following these restrictions, the translation has four phases, each discussed in detail in subsequent paragraphs:

(i) provision of program variables,
(ii) generation of assumptions and safety condition,
(iii) control code generation,
(iv) provision of ODEs and constraints.

### 5.3.1 Program Variables
For each field, parameter, and local variable in \(c\) we create a program variable with the same name. For each method \(m\) we create a time variable \(t_m\), for each in-port method \(m\) a tick variable \(tck_m\), both type \(\text{Real}\); \(tck_m\) models the unknown time when an in-port method is called next. Time variables are local time for each method and determine when a time-triggered controller or an in-port is executed the next time. We denote the set of all tick variables with Tick and the set of all time variables with Time.

### 5.3.2 Assumptions and Safety Condition
The formula \(\text{assumptions}_C\) (2) is \(C\)'s precondition \(\text{pre}\) plus all initializations init plus conditions on the time and tick variables: in the beginning, each time variable starts at zero and the tick variable has an unknown positive value. Each tick variable \(tick\) has a method \(\varphi_{\text{tick}}\) that is responsible for its generation. We refer to the timed input requirement of this method with \(\psi(tick)\), where the method name \(\varphi_{\text{tick}}\) has been replaced with \(tick\). The initial value of the tick variable is also described by the timed input requirement and describes when the method is issued for the first time at the latest.

\[
\text{assumptions}_C \equiv \text{pre} \land \bigwedge_{\varphi \in \text{init}} \varphi \land \bigwedge_{t \in \text{Time}} t = 0 \land \bigwedge_{\text{tick} \in \text{Tick}} (0 < \text{tick} \land \psi(\text{tick}))
\]

The formula \(\text{safety}_C\) (3) captures the guarantees of class \(C\): we need to show that \(C\)
(i) preserves its own invariant \(\text{inv}\);
(ii) provides guarantees \(\text{Ens}\) about own out-port methods (shows what others can rely on);
(iii) respects timed preconditions \(\text{Req}^*\); and,
(iv) when writing to in-port methods of callees, respects their input requirements \(\text{Req}^*\).

If class \(c\) comes with a time-triggered controller with guard \(\text{duration}(e, e)\), technical constraint 5.3(1) above ensures that at the moment the controller calls an in-port of another object, it has a correct copy of the callee state. \(\text{Req}^*\) are input requirements of used in-port methods of
other classes than C, where the method parameter is replaced by the field passed to it. Ens are guarantees of all out-port methods of C. Some special care needs to be taken for timed input requirements. With TReq, we denote the set of timed input requirements (constructed over tick, as above) of all called in-ports where such a clause is given.

\[ \text{safety}_C \equiv \text{inv} \wedge \bigwedge_{\varphi \in \text{Req}} \bigwedge_{r \in \text{TReq}} \bigwedge_{\psi \in \text{Ens}} \varphi \wedge r \wedge \psi \]  

(3)

The safety condition expresses that the controllers of class C respect the input requirements when writing to the in-port methods of other components and call in-port methods with a timed input requirement sufficiently open. The structure of controllers in CHABS per Sect. 3.3 enforces that these calls occur last in the controller bodies.

### 5.3.3 Control Code

The translation of ABS statements to hybrid programs is defined in Fig. 20. We discuss the non-obvious rules: Calls e!m() to in-port methods of other objects are mapped to ?true (i.e. skip), because there is no effect on the caller object. A read f=e.m() from an out-port method is mapped to \trans(f) := ?true; ?e.m: a non-deterministic assignment, restricted with a subsequent test for the guarantee of the called out-port method.

The translation of ports and control methods has the general form if (check) then \{exec, cleanup\}. This pattern is instantiated per method type as follows:

- Time-triggered controller \( m \) with method body \( \text{await duration}(e, e); s; \text{this.m}() \): check makes sure the correct duration elapsed and cleanup resets time, so check \( \equiv t_m := \trans(e), \) exec \( \equiv \trans(s), \) cleanup \( \equiv t_m := 0. \)

- Event-triggered controller \( m \) with method body \( \text{await diff } e; s; \text{this.m}() \): check tests the guard, so check \( \equiv \trans(e), \) exec \( \equiv \trans(s), \) cleanup \( \equiv ?true. \)

- In-port method \( m \) with body \( \text{this.f} = v, \) input requirement \( \varphi \) and timed input requirement \( \psi \): check ensures the correct duration elapsed, so check \( \equiv t_m := \text{tick}_m; \) exec chooses a value consistent with \( \varphi, \) so exec \( \equiv f := ?\varphi; \) finally, cleanup does the same for a new duration consistent with \( \psi \) (method name replaced by \text{tick}_m), so cleanup \( \equiv \text{tick}_m := ?\varphi; \text{tick}_m > 0; ?\psi; t_m := 0. \)

- Out-port methods and the run method are not translated. Out-port methods have no effect on object state and their guarantees (included in (1) in safety\(_C\)) must be shown to hold throughout plant execution. The run method initializes the system and ensures that every controller can run once before the first plant execution, which is guaranteed in (1) through sequential composition of code\(_C;\) plant\(_C\).

Let \( M \) be the set of all translations of in-port methods and controllers, then:

\[ \text{code}_C \equiv \left( \sum \prod M \right) \left( \sum M \right)^* \]  

(4)

The controller code\(_C\) first executes all controllers in a non-deterministically chosen order \( \left( \sum \prod M \right), \) then allows each controller/in-port to repeat \( \left( \sum M \right)^* \). The latter replicates eager ABS behavior on satisfied guards: when an event-triggered controller is triggered and its guard still holds after its execution, then in ABS the controller is run again.

Note that \( \left( \sum M \right)^* \) safely overapproximates all possible orders, including the behavior of the first part \( \sum \prod M \). However, including \( \sum \prod M \) in code\(_C\) simplifies practical proofs, because in typical models that disable the check guards at the end of control and in-port method bodies (e.g., a time-triggered controller that resets time in cleanup so that it becomes re-enabled only after some time passes), every method is executed at most once before time advances. The structure of the controller code\(_C\) mirrors this with the first part \( \sum \prod M \) to simplify practical proofs as follows:
(i) the proof obligations of enabled control and in-port methods (i.e., whose check is true) are
easier because the outer loop is dropped, and additionally the proof obligations of all the
disabled control and in-port methods can be easily disposed of by contradiction with their
check guards;
(ii) finding a loop invariant for the second part \((\sum M)^+\) is easy when no method is executed
twice before time advances: in that case, the loop invariant for \((\sum M)^+\) must simply imply
that none of the check guards holds.

Further note that \(\sum \prod M\) does not exclude runs, because the general form

\[
\text{if (check) then \{exec; cleanup\}}\]

of control methods and ports in \(M\) ensures that there is
progress through the implicit else ?true even if all controllers and in-ports are disabled.

5.3.4 Plant

The plant of a class \(C\) has the form

\[
\text{plant}_C \equiv \sum \{(\text{ode}, \text{ode}_t, c) \mid c \in C\},
\]

where \(\text{ode}\) is the ODE from its physical block, \(\text{ode}_t\) describes the time variables, and the constraints
\(c \in C\) partition the domain of the physical fields. The boundaries of the subdomains overlap
exactly where the differential guards hold.\(^7\) This models guards as events in \(dL\), following the
modeling pattern described in Sect. 5.1. To ensure that no differential guard is omitted, it is
necessary that no two differential guards share a program variable. This is not a restriction, as
two controllers can be merged with a disjunction: see the guard in Fig. 2.

To define \(C\) let \(e_1, \ldots, e_m\) be the translations of differential guards in the class and \(\tilde{e}_i\) the weak
complement of \(e_i\). Let \(t_1, \ldots, t_l\) be all time variables introduced for time-triggered controllers with
\(e_t\), the expression in the duration statement. Let \(p_{t1}, \ldots, p_{tk}\) be all time variables introduced for
in-port methods and \(\text{tick}_{pt}\) the associated tick variable. We set \(\text{ode}_t \equiv \{t_1 = 1, \ldots, t_l = 1, p_{t1} = 1, \ldots, p_{tk} = 1\}\) and define:

\[
\mathcal{C} \equiv \{(e_1, \tilde{e}_1) \times \{e_2, \tilde{e}_2\} \times \cdots \times \{e_m, \tilde{e}_m\}\}
\]

\[
\cup \{t_1 \leq e_t, t_1 \leq \text{tick}_{pt}, t_1 \leq \text{tick}_{pt}, t_1 \leq \text{tick}_{pt}\} \cup \{p_{t1} \leq \text{tick}_{pt}, p_{t1} \leq \text{tick}_{pt}\} \cup \{p_{t1} \leq \text{tick}_{pt}, p_{t1} \leq \text{tick}_{pt}\} \cup \{p_{t1} \leq \text{tick}_{pt}, p_{t1} \leq \text{tick}_{pt}\}.
\]

5.3.5 On the Random Number Generator

We do not translate the \(\text{random}(i)\) expression from HABS to \(dL\), because its semantics is that it
returns an integer below \(i\). However, integer arithmetic is undecidable, which is the reason why \(dL\)
opts to embed its modality into a decidable first-order logic over the reals [66]. A straightforward
overapproximation with a translation to a variation of \(\text{random}\) that returns a real value is:

\[
\text{trans}(f = \text{random}(r)) \equiv \text{trans}(f) := \ast; ?(0 \leq \text{trans}(f) < \text{trans}(r))
\]

5.4 Compositional Verification

We can now state our main theorem: If we can prove safety of all classes, i.e., close all proof
obligations, then the whole system is safe, i.e., every class indeed preserves its invariant. Verification
is compositional: if we change the code or invariant of one class, only the proof obligation of this
class has to be reproofed. If we change a method precondition, additionally the proof obligations
of all calling classes have to be reproofed.

\(^7\) Expressions contain only \(>=, <=\), so weak complement ensures a boundary overlap.
Theorem 5. Let \( P \) be a set of classes, with each \( C \in P \) associated with \( \varphi_C \) per formula (1). If all the \( \varphi_C \) are valid, then for every main block that creates objects satisfying \( \text{pre}_C \) all reachable states of all objects satisfy \( \text{inv}_C \).

Proof Sketch. Recall that the trace of an HAO is an assignment of time to stores (Def. 4). For the proof, each store is indexed by its time and the trace starts with 0 (i.e., the possible offset caused by the delayed object creation is removed):

\[
\theta_o(t) = (\rho_i)_{i \in \mathbb{R}^+} = \rho_0 \cdots
\]

We are going to use that there are only countably many discrete steps in a run and partition the trace into countably many subtraces. Then we show by induction on these discrete steps that the invariant is always preserved.

Let \( D \) be the set of all time points with discrete steps of \( o \) in the run that generates \( \theta_o \). Note that \( 0 \in D \) and that \( \theta_o(d) \) is the last store defined by the SOS semantics, if several such stores share the same time; further note that this is reflecting the reachability relation of \( d\mathcal{L} \).

We define \( \theta^d_o \) as the subtrace of \( \theta_o \) starting with \( d \) and ending at the next time point of a discrete step. Let \( \text{next}(d) \) be the next time point of a discrete step after \( d \), if such a time point exists, and \( \infty \) otherwise:

\[
\text{dom} \left( \hat{\theta}^d_o \right) = [d..\text{next}(d)] \quad \text{with} \quad \hat{\theta}^d_o(t) = \theta_o(t)
\]

We observe that each state in the \( \text{HABS} \) semantics is also a state in the Kripke structure of the semantics if all class parameters are removed. We show that \( \text{trans} \) preserves reachability: if from a state \( \rho \) state \( \rho' \) is reachable by an \( \text{HABS} \) statement \( s \) in the \( \text{HABS} \) semantics, then state \( \rho' \) is reachable from state \( \rho \) by \( \text{trans}(s) \). This is justified as follows:

1. The \( d\mathcal{L} \) program omits no events, because each event is at a boundary of two evolution domain constraints on a variable and no two events share a variable (each controller has its own time variable).
2. The evolution domain constraints cover all possible states, so no run is rejected for a domain being too small.
3. Each test in \( d\mathcal{L} \) formula \( \varphi_C \) that discards runs does so using a condition that is provably guaranteed by other objects. For example, the test that discards all runs of an in-port method for inputs not satisfying its input requirements is safe, because on the caller side this condition is part of the safety condition (3).
4. The observation also relies on technical constraint (1) above and the recursive call being at the end of a controller. Together, this guarantees that \textit{at that moment} the caller copy of the callee’s state is consistent with the callee’s actual state.

Let \( D = (d_i)_{i \in \mathbb{N}} \) be an enumeration of the discrete time points and \( \hat{\theta}^d_i \) the union of all subtraces of \( \theta_o \) up to \( d_i \):

\[
\text{dom} \left( \hat{\theta}^d_i \right) = \bigcup_{j \leq i} \text{dom} \left( \theta^j_o \right) \quad \text{with} \quad \hat{\theta}^d_i(t) = \theta_o(t)
\]

We show by induction on \( i \) that every state in \( \hat{\theta}^d_i \) is safe, i.e., a model for the invariant \( \text{inv}_C \).

Induction Base: \( i = 0 \). It is explicitly checked that \( \theta^0_o \) is safe. By assumption, the object is created in a state \( \theta^0_o \) such that the precondition \( \text{pre}_C \) holds. From axiom 1 of \( d\mathcal{L} \) \cite{68} we know that the safety condition must be true in the beginning of the loop, thus validity of \( \varphi_C \) implies validity of \( \text{pre}_C \rightarrow \text{inv}_C \). Since all the formulas \( \varphi_C \) are proved in isolated component proofs, we conclude \( \text{inv}_C \) holds for all reachable states of all objects as by the correctness argument reachability is preserved.
Induction Step. $i > 0$. This is analogous to the base case, but instead of an explicit check that $d_i$ is safe, we use the induction hypothesis that every state in $\hat{\theta}^{d_{i-1}}$ is safe and that the statement for $d_i$ is executed in a state at time $t \in \text{dom} (\hat{\theta}^{d_{i-1}})$.

Remark. The theorem states soundness of safety properties in $d\mathcal{L}$ proof obligations and does not prove semantic equivalence between the contained $d\mathcal{L}$-program and the HABS class. This approach stands in the tradition of modular deductive verification of object-oriented software, in particular, it follows the structure of systems for distributed object-oriented programs [52]. The main reason to pursue this approach is that the form of proof obligations and the translation of statements cannot be disentangled: the translation of method calls includes the postcondition of the called methods: soundness of the translation relies on the fact that all other proof obligations can be established. This is already the case for discrete, sequential languages [41]. Note that this is not circular. As the proof of Theorem 5 shows, we can order all method executions in a run such that we have a well-founded induction on them. The first method execution in every object relies only on the state precondition which is guaranteed at creation. These in turn are guaranteed in the main block, which has no assumptions. Another reason is that each $d\mathcal{L}$ proof obligation corresponds to the (symbolic) execution of one object in a class. To model all permissible evolutions of several method executions in a proof, therefore, it is necessary to encode the scheduler. This requires a form of proof obligation that assumes the object invariant (which contains scheduling constraints). This effect is well-known in deductive verification of distributed programs [31, 32, 52].

5.5 Case Study

We illustrate the HABS-to-KeYmaera X translation defined above with the TankTick system in Fig. 4. The example, the implementation of the translation and the simulation, as well as the mechanical proofs of the translation are available in the supplementary material.

5.5.1 Class CTank

The in-port method inDrain() of the CTank class gives rise to a time variable $t_{\text{inDrain}}$ and a tick variable $\text{tick}_{\text{inDrain}}$. Following (2), assumptions$\text{Tank}$ is:

$$\text{assumptions}_\text{Tank} \equiv 4 \leq \text{inVal} \leq 9 \quad \land \quad t_{\text{inDrain}} = 0 \land 0 < \text{tick}_{\text{inDrain}}$$

$$\land \quad \text{level} = \text{inVal} \land \text{drain} = -1/2 \quad (6)$$

The safety condition says the tank level stays within its limits and that level adheres to its contract which happen to be identical. No in-port methods of other classes are used, hence:

$$\text{safety}_\text{Tank} \equiv 3 \leq \text{level} \leq 10 \quad . \quad (7)$$

The CTank class has no controller method, so the inDrain method, which has a timed input requirement, per (4) results in code$\text{Tank}$ below

$$\text{code}_\text{Tank} \equiv p; (p)^4 \quad (8)$$
where \( p \equiv \text{trans}(\text{inDrain}) \) below is translated from Fig. 4 using the translation of Fig. 20:

\[
p \equiv \text{if } (\text{inDrain} \models \text{tick}_{\text{inDrain}}) \text{ then } \\
\text{drain} := *; \\
? -1/2 \leq \text{drain} \leq 1/2 \land (\text{drain} < 0 \rightarrow \text{level} \geq 3.5) \\
\land (\text{drain} > 0 \rightarrow \text{level} \leq 9.5); \\
\text{tick}_{\text{inDrain}} := *; \ ? < \text{tick}_{\text{inDrain}} < 1; \ \text{inDrain} := 0
\]

The plant \( \text{plant}_{\text{Tank}} \), following shape (5), is based on the physical block and the new clock variable (there are no differential guards), with the evolution domain constraint split along the new time variable \( t_{\text{inDrain}} \). ODEs of the form \( v' = 0 \) are default and omitted.

\[
\begin{align*}
\text{plant}_{\text{Tank}} & \equiv \text{plant}_{\text{Tank}}^< \cup \text{plant}_{\text{Tank}}^> \\
\text{plant}_{\text{Tank}}^< & \equiv \{ \text{level}' = \text{drain}, \ t_{\text{inDrain}}' = 1 \land t_{\text{inDrain}} \leq \text{tick}_{\text{inDrain}} \} \\
\text{plant}_{\text{Tank}}^> & \equiv \{ \text{level}' = \text{drain}, \ t_{\text{inDrain}}' = 1 \land t_{\text{inDrain}} \geq \text{tick}_{\text{inDrain}} \}
\end{align*}
\]

**Lemma 6.** Class \( \text{Tank} \) is safe, i.e., formula \( \forall_{\text{Tank}} \) — obtained per (1) referring to tank assumptions \( \text{assumptions}_{\text{Tank}} \) (6), postcondition \( \text{safety}_{\text{Tank}} \) (7), code \( \text{code}_{\text{Tank}} \) (8), and plant \( \text{plant}_{\text{Tank}} \) (9) — is valid.

\[
\forall_{\text{Tank}} \equiv \text{assumptions}_{\text{Tank}} \rightarrow [(\text{code}_{\text{Tank}}; \ \text{plant}_{\text{Tank}})^*] \text{safety}_{\text{Tank}}
\]

**Proof.** See KeYmaera X proofs in the supplementary material. The proof sketch here serves as an illustration of how sequent proofs in KeYmaera X systematically use the invariant annotations in HABS. In the proof, we show the inductive loop invariant \( \text{inv}_{\text{Tank}}^< \) which expresses that the level always stays within limits and that the next input will be supplied before exceeding the timed input requirement as follows: \( 3 \leq \text{level} \leq 10 \land -1/2 \leq \text{drain} \leq 1/2 \land 3 \leq \text{level} + \text{drain}(\text{tick}_{\text{inDrain}} - t_{\text{inDrain}}) \leq 10 \land \text{tick}_{\text{inDrain}} \leq t_{\text{inDrain}} \).

The proof starts in step \( \rightarrow_R \) to make the left-hand side \( \text{assumptions}_{\text{Tank}} \) of the implication available as assumptions. Next, \([\cdot] \) uses the loop invariant \( \text{inv}_{\text{Tank}}^< \) for induction: the base case in the left-most subgoal and the use case in the right-most subgoal follow by real arithmetic automation; the induction step in the middle subgoal continues with \([\cdot] \) to split the sequential composition into nested box modalities.
The main insight now is that \texttt{codeTank} reacts at the latest when \texttt{tickInDrain} = \texttt{tInDrain} and will reset the timer using \texttt{tickInDrain} := 0, so that the timing requirement \texttt{tickInDrain} ≤ \texttt{tInDrain} can be strengthened to a strict inequality \texttt{tickInDrain} < \texttt{tInDrain} in the inductive loop invariant. The resulting intermediate condition \texttt{invTank} is used in step MR to split into two subgoals: in the left subgoal of MR, we show that \texttt{codeTank} guarantees the intermediate condition \texttt{invTank} < \texttt{tInDrain}. In the right subgoal of MR we show that \texttt{plantTank} preserves the loop invariant from that intermediate condition: the plant listens for the event \texttt{tickInDrain} = \texttt{tInDrain} with a choice between two differential equations, whose evolution domain constraints exactly overlap at the event. On evolution domain \texttt{tickInDrain} ≤ \texttt{tInDrain} in \texttt{plantTank}, the differential equation preserves the loop invariant, whereas on evolution domain \texttt{tickInDrain} ≥ \texttt{tInDrain} in \texttt{plantTank} the contradiction shows that the controller reacts such that the plant can never enter this unsafe behavior. ▶

5.5.2 Time-Triggered Controller \texttt{FlowCtrl}

Assumptions \texttt{assumptionsFlowCtrl} of \texttt{FlowCtrl} constructed per (2) and plant \texttt{plantFlowCtrl} constructed per (5) are straightforward. The latter is created for the sake of observing time events, even though no physical block is present:

\begin{align}
\text{assumptionsFlowCtrl} & \equiv 0 < \texttt{tick} < 1 \\
\text{plantFlowCtrl} & \equiv \{t'_{\text{ctrlFlow}} = 1 \& t_{\text{ctrlFlow}} \geq \texttt{tick}\} \\
& \quad \cup \{t'_{\text{ctrlFlow}} = 1 \& t_{\text{ctrlFlow}} \leq \texttt{tick}\}
\end{align}

The safety condition \texttt{safetyFlowCtrl} constructed per (3) is the timed input requirement of the called \texttt{inDrain} method and the class invariant (subsumed by the input requirement of \texttt{inDrain}):

\begin{align}
\texttt{safetyFlowCtrl} & \equiv -1/2 \leq \texttt{drain} \leq 1/2 \land \texttt{tick} < 1 \\
& \quad \land (\texttt{drain} < 0 \rightarrow \texttt{level} \geq 3.5) \\
& \quad \land (\texttt{drain} > 0 \rightarrow \texttt{level} \leq 9.5)
\end{align}

Finally, the code \texttt{codeFlowCtrl} is translated as

\begin{align}
\texttt{codeFlowCtrl} & \equiv q; (q)^* 
\end{align}

with

\begin{align}
q & \equiv \text{if } (t'_{\text{ctrlFlow}} = \texttt{tick}) \text{ then} \\
& \quad \text{level} := *; ?'3 \leq \texttt{level} \leq 10; \\
& \quad \text{if } (\texttt{level} \leq 3.5) \text{ then } \{\texttt{drain} := 1/2\}; \\
& \quad \text{if } (\texttt{level} \geq 9.5) \text{ then } \{\texttt{drain} := -1/2\}; \\
& \quad t_{\text{ctrlFlow}} := 0
\end{align}

\textbf{Lemma 7.} Class \texttt{FlowCtrl} is safe, i.e., formula \(\varphi_{\text{FlowCtrl}}\) — obtained per (1) referring to assumptions \texttt{assumptionsFlowCtrl} (10), postcondition \texttt{safetyFlowCtrl} (12), code \texttt{codeFlowCtrl} (13), and plant \texttt{plantFlowCtrl} (11) — is valid.

\(\varphi_{\text{FlowCtrl}} \equiv \text{assumptionsFlowCtrl} \rightarrow [(\texttt{codeFlowCtrl}; \texttt{plantFlowCtrl})^*] \texttt{safetyFlowCtrl}\)

\textbf{Proof.} See KeYmaera X-proofs in the supplementary material. ▶
5.5.3 Event-Triggered Controller CSingleTank

Translation of class CSingleTank from Fig. 2 illustrates the handling of event-triggered controllers. The plant and code interact. The plant separates the evolution domain into two parts, with the guard of the event-triggered controller (the white areas in Fig. 21) defining their boundary. The gray areas are larger than the safe region defined by $3 \leq \text{level} \leq 10$. This is necessary to avoid Zeno behavior in the eager execution semantics of HABS: If we used simply the weak complement of the safe region $\text{level} < 3 \lor \text{level} > 10$ as a guard and happen to be in a program state at the boundary (the lower of the states indicated with a star in Fig. 21), then the controller changes the state as shown by the arrow. But if the next state is again on the boundary, which is the case when the safe region is too small, then the guard is triggered, the controller loops back to the first state, etc., without physical time being able to advance. The guard in Fig. 2 ensures that after the controller has run, the state is not on the boundary anymore. This behavior is exhibited by our implementation, see Fig. 3. The code codeCSingleTank has the form $r; (r)^*$ with $r$ being:

$$r \equiv \text{if } (\text{level} \leq 3 \land \text{drain} \leq 0) \lor (\text{level} \geq 10 \land \text{drain} \geq 0) \text{ then}$$

$$\text{if } (\text{level} \leq 3) \text{ then } \text{drain} := 1/2 \text{ else } \text{drain} := -1/2$$

The plant of CSingleTank with sufficiently large regions is as follows:

$$\text{plant}_{\text{CSingleTank}} \equiv$$

$$\{ \text{level}' = \text{drain} \land (\text{level} \leq 3 \land \text{drain} \leq 0) \lor (\text{level} \geq 10 \land \text{drain} \geq 0) \}$$

$$\cup \{ \text{level}' = \text{drain} \land (\text{level} \geq 3 \lor \text{drain} \geq 0) \land (\text{level} \leq 10 \lor \text{drain} \leq 0) \}$$

5.6 On Translation into $dL$

HABS programs can be tested and validated, but the programmer needs to avoid writing programs that are
1. inherently difficult to interpret and
2. have a high degree of non-determinism.

Both are good programming and software engineering practices, of course, and the fact that HABS is a programming language enables one to apply standard techniques for discrete programs.

A back-translation from $dL$ to HABS would provide meaningful validation only for deterministic $dL$ models. While being possible even in the general case, two traits of $dL$ programs prohibit easy interpretation and simulation:

Highly Non-Deterministic Structure Additionally to non-deterministic assignment, branching and repetition are both non-deterministic: the – rather non-intuitive – representation of $(a)^*$ in HABS is a loop that non-deterministically chooses to break out.

```plaintext
1 while(True) {
2     Int i = random(2);
3     if (i == 1) break;
4     s;
5 }
```
This loop may never terminate, while the semantics of $d\mathcal{L}$ loops defines an arbitrary but countable number of repetitions. A similar pattern has to be employed for branching.

Tests The test $?\phi$ discards a run based on a $d\mathcal{L}$-guard. Translation would require
1. to evaluate $d\mathcal{L}$ formulas, as opposed to Boolean expressions, and
2. a mechanism to abort the program.
This can be emulated by exceptions, but it obfuscates the semantics.

6 Related & Future Work, Conclusion

6.1 Related Work

Previous work on hybrid programming concentrated on purely sequential languages: HybCore [39] is a while-language with hybrid behavior and a simulator [40], but lacks formal verification techniques. Its extensional semantics is not able to express the timed properties needed for our distributed controller. While $dt$ [77] is also a while-language and uses infinitesimals instead of ODEs to model continuous dynamics. It has a simple verification system based on Hoare triples [42], but is not executable.

Hybrid Rebeca (HR) [46] proposes to embed hybrid automata directly into the actor language Rebeca. In contrast to HABS, no simulation is available and verification is not object-modular: the whole model is translated to a single monolithic hybrid automaton. Because of this, a number of boundedness constraints have to be imposed. The translation is also the semantics: HR has no semantics beyond this translation and is mainly a frontend for Hybrid Automata tools. The verification backend of HR does not support non-linear ODEs (our examples are linear, but HABS, KeYmaera X, and Maxima, support non-linear ODEs; HABS models with non-linear ODEs are found in the online supplement).

Recent efforts [58, 64] split the verification task in $d\mathcal{L}$ into manageable pieces by modularizing deductive hybrid systems verification with component-based modeling and verification techniques, but impose strict structural requirements on components and communication. The Sphinx modeling tool [62] for $d\mathcal{L}$ represents non-distributed hybrid programs with UML class and activity diagrams, but for verification purposes it translates these model artifacts into a single monolithic hybrid program.

The Architecture Analysis and Design Language (AADL), a language to model hardware and software components in embedded systems, has a hybrid extension [2], which uses the HHL [80] theorem prover as its verification backend [1]. HHL is based on Hoare triples over hybrid CSP programs and duration calculus formulas [57]. Hybrid AADL offers structuring elements for components and their connections on the architecture level. The semantics of hybrid AADL is given as a translation of the synchronous fragment of AADL into hybrid CSP, while we extend the semantics of the actor-based programming language ABS to combine reasoning about the asynchronous behavior of communicating components in ABS with reasoning about the internal combined discrete and continuous component behavior in differential dynamic logic. As a side effect, the extended semantics enables proving the correctness of the translation to differential dynamic logic, as well as translating HABS to other formal languages.

A similar approach based on Stateflow/Simulink is implemented in the MARS toolkit [22]. The MARS approach is orthogonal to HABS: MARS connects a verification toolkit around a simulation language (which is a daunting task given the missing formal semantics of Stateflow/Simulink), while HABS is designed specifically to enable verification and simulation through its languages features. This is reflected in the soundness proof, which is based on a bidirectional translation.

Another approach based on CSP and the duration calculus combines these formalisms with Object-Z [45]. This enables model-checking for real-time systems (clocks with resets), while we support hybrid systems theorem proving with (non-linear) differential equations. A further integration of Object-Z and (Timed) CSP was investigated by Mahony & Dong [60].
Hybrid Event-B [12, 13] extends Event-B refinement reasoning with continuous behavior between the usual discrete Event-B events. A more lightweight approach [76, 21] models hybrid systems in an abstract way as action systems without differential equations directly in Event-B, and complements analysis in Event-B with simulation in Matlab. Similarly, Dupont et al. [34] use Event-B for a correct-by-construction approach to hybrid systems. They embed the ODEs used for continuous modeling by declaring them as a special theory within Event-B instead of extending the core language itself.

Integrated tools such as Ptolemy [71], Stateflow/Simulink except the aforementioned MARS toolkit, and Modelica, all emphasize simulation, reachability analysis (e.g., CHARON [6, 7], Ariadne [15]), or testing (e.g., [30]). As supporting techniques, they provide modeling notation for timing aspects, signals, and data flow between heterogeneous models. Formal verification of hybrid systems with reachability analysis and model checking tools (SpaceEx [35], CORA [4], Flow* [23]) support modularity [33] based on hybrid I/O automata [59], assume-guarantee reasoning [17, 43], and hybridization [24]. However, they work best for finite-horizon analysis and finite regions (because over-approximations stay tight only for bounded time and from small starting regions). Similar restrictions apply to dReal/dReach [37, 55].

Dynamic I/O automata [9] for modeling dynamic systems introduce a notion of externally visible behavior, the ability to create and destroy automata and change their signature dynamically; those features are all naturally available in our object-oriented approach and do not need special extension like automata-based modeling tools. Our work contrasts with all mentioned simulation and verification approaches by providing a uniform modeling language, validation by simulation, modular infinite-horizon and infinite-region theorem proving through translation from HABS to dL.

Translation among hybrid system languages so far centers around hybrid automata as a unifying concept [11, 79]. Others focus on the discrete fragment [38]. Our translation from HABS to dL translates complete hybrid system models written in a programming language, including annotations (preconditions, invariants, etc.). It is sound relative to the formal semantics of HABS and dL.

Hybrid systems validation through simulation is addressed with translation to Stateflow/Simulink [10]; with a combination of discrete-event and numerical methods [19]; and with co-simulation between control software and dedicated physics simulators [26, 78, 82]. Here, we focus on safety verification, the distributed aspect of HABS models, and take a pragmatic first step for simulating continuous models.

In summary, HABS is designed for modular deductive verification (unlike simulation-centric tools), infinite-horizon analysis on infinite regions (unlike reachability analysis and model checking tools), without sacrificing high-level programming language features (unlike hybrid systems modularization techniques and assume-guarantee reasoning).

### 6.2 Future Work

The present work lifts the research on formal semantics of programming languages for hybrid systems from verification-centric minimalistic languages to distributed object-oriented languages. Carrying over techniques, ideas, and analyses from programming language research to hybrid systems programming, presents an intriguing research direction. Our ongoing work on larger case studies with HABS, in particular in connection with co-simulation [54], is expected to reveal additional challenges.

We plan to combine the verification of CHABS presented here with the more modular approach based on post-regions [51], which does not support timed input requirements yet. Future research avenues include investigating how the static analyses for ABS, in particular the deadlock analysis for
boolean guards [50], can be extended for HABS, extending approximate simulation of non-solvable differential equations, experimenting with various computer algebra systems, and supporting guards with non-urgent semantics.

6.3 Conclusion

Distributed hybrid systems are not only difficult to verify formally, it is equally hard to validate a formal model of them, especially with components using symbolic computations, such as servers. Both activities have conflicting demands, so we propose a translation-based approach: modeling is guided by patterns over hybrid programs and class specifications in HABS, a hybrid extension of the concurrent active-object language ABS. These are automatically decomposed and translated (Thm. 5) into sequential proof obligations of the verification-oriented differential dynamic logic dL and discharged by the hybrid theorem prover KeYmaera X.

We illustrated the viability of our approach by a case study that features many complications: concurrent behavior, possible non-termination, correctness depending on timing constants, multi-dimensional domain, time lag in sensing, etc.

References


A Hybrid Programming Language for Formal Modeling and Verification of Hybrid Systems


