Model Checking Implantable Cardioverter Defibrillators

Houssam Abbas, Kuk Jin Jang, Zhihao Jiang, Rahul Mangharam
Department of Electrical and Systems Engineering
University of Pennsylvania, Philadelphia, PA, USA
{habbas, jangkj, zhihaoj, rahulm}@seas.upenn.edu

ABSTRACT

Ventricular Fibrillation is a disorganized electrical excitation of the heart that results in inadequate blood flow to the body. It usually ends in death within a few seconds. The most common way to treat the symptoms of fibrillation is to implant a medical device, known as an *Implantable Cardioverter Defibrillator* (ICD), in the patient's body. Model-based verification can play a crucial role in ICD development. In this paper, we build a hybrid system model of the human heart+ICD closed-loop system, and show that it admits a finite bisimulation by showing it to be a STORMED hybrid system. In general, it may not be possible to compute the bisimulation. We show that approximate reachability can yield a finite *simulation* for STORMED systems, which improves on the existing verification procedure. In the process, we show that certain compositions respect the STORMED property. Thus it is possible to model check important formal properties of ICDs in a closed loop with the heart, such as delayed therapy, missed therapy, or inappropriately administered therapy. The results of this paper are theoretical, since no model checkers exist for STORMED systems. In future work we will implement a procedure for model checking the heart+ICD loop.

1. INTRODUCTION

Implantable Cardioverter Defibrillators (ICDs) are life-saving medical devices. An ICD is implanted under the shoulder, and connects directly to the heart muscle though two electrodes and continuously measures the heart's rhythm (Fig. 1). If it detects a potentially fatal accelerated rhythm, the ICD delivers a high-energy electric shock or sequence of pulses through the electrodes to reset the heart's electrical activity. Without this therapy, this *tachycardia* is usually fatal within seconds of onset. In the US alone, 10,000 people receive an ICD every month. Studies have presented evidence that patients implanted with ICDs have a mortality rate reduced by up to 31% [13].

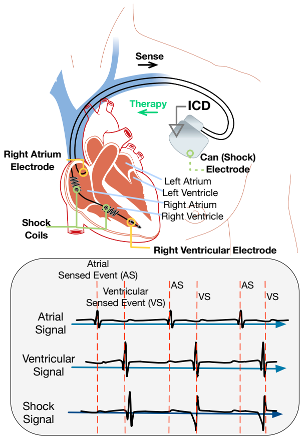


Figure 1: ICD connected to a human heart via two electrodes. The ICD monitors three electrical signals (known as electrograms) traversing the heart muscle.

Unfortunately, ICDs suffer from a high rate of *inappropriate therapy* due to poor detection of the current rhythm on the part of the ICD. Inappropriate shocks increase patient stress, reduce their quality of life, and are linked to increased morbidity [16]. Depending on the particular ICD and its settings, the rates of inappropriate therapy range from 46% to 62% of all delivered therapy episodes [7]. Current practice for ICD verification relies heavily on testing and software cycle reviews. With the advent of computer models of the human heart, *Model-Based Design* (MBD) can and should play a prominent role in ICD development. This paper presents hybrid system models of the human heart and of the common modules of ICDs currently on the market, and shows that the closed loop formed by these models is *formally verifiable.* The objective is to develop model checkers for ICDs to further their MBD process.

Earlier work on verification of medical devices (formal or otherwise) focuses on pacemakers. In [9] the authors developed timed automata models of both heart and pacemaker, which allows formal verification of LTL properties of the heart+pacemaker loop. In [5] the authors perform probabilistic testing-based verification of Hybrid I/O automata models of heart and pacemaker. However, they can not be symbolically verified. Later work on pacemakers [12] develops a formalized cellular automata (CA) model of the heart and uses Event-B for expressing its properties. CA-based models [2],[12] are appealing due to their intuitive correspondence with the heart's anatomy and function and their relative computational simplicity.

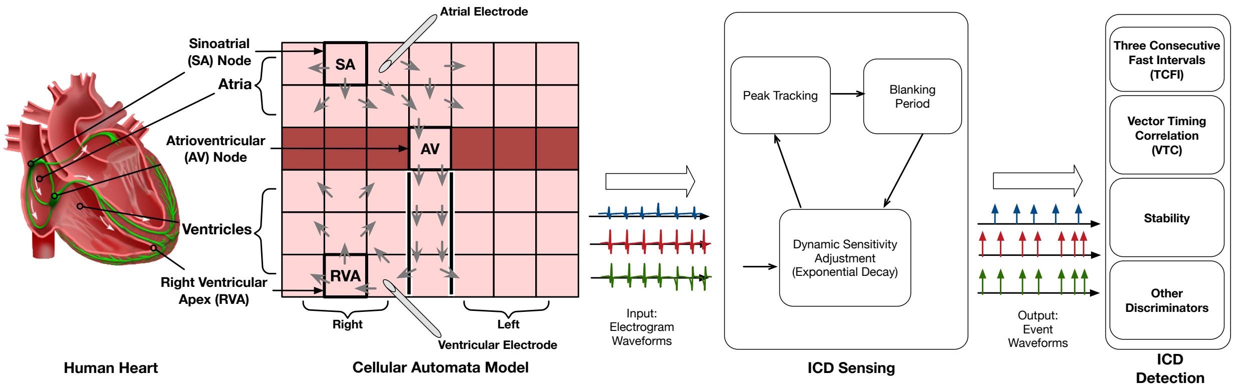


Figure 2: The whole heart is modeled as a 2D mesh of cells (Section 3). The ICD electrodes are shown in the right atrium and ventricle. The electrogram signals measured through the electrodes are processed by the sensing module (ICD Sensing, see Section 4). The detection algorithm (Section 5) determines the current rhythm using the processed signal (ICD Detection). AV: atrio-ventricular node, RVA: right ventricle apex, SA: sino-atrial node.

The ICD algorithms are more complex than a pacemaker's: an ICD measures the timing of events, but also measures and processes the *morphology* of the electrical signal in the heart to distinguish many types of arrhythmias. Thus, we need three models for ICD verification: a timing and voltage model of the heart, a model of the ICD's algorithms, and a model for voltage measurement by the ICD electrodes. This takes the model out of the realm of timed automata and into hybrid automata proper.

The first contribution of this paper is to develop a hybrid system model of the heart, the ICD measurement process, and of the algorithmic components of ICDs from most major manufacturers on the market. We show that the composition of these three models can be *formally verified*: specifically, it admits a finite bisimulation [1]. The ICD models presented here are the first formalization of ICD operation to the best of our knowledge.

To establish this result we use the theory of STORMED hybrid systems [23], a class of hybrid systems that have finite bisimulations. Our second contribution is two general results for STORMED systems. First we prove that parallel compositions of STORMED systems yield STORMED systems. Secondly, we show that any (definable) over-approximate reach tubes can replace the exact flows of a STORMED system, yielding a system that still admits a finite simulation (but no longer a bisimulation). Finally, we show that the reach sets computed by the reachability tool SpaceEx [6] are definable and so can be used to build the simulation.

Our interest in not simply in a particular manufacturer's arrhythmia detection algorithm: rather, we are interested in those components that are common to most of them, thus making our results relevant to them. The components we model or some variation on them are included in the ICDs of Boston Scientific, Medtronic, Saint-Jude Medical and Biotronik. This is the first example of a practical STORMED system that the authors are aware of. In future work we will implement a model checker for this type of systems in order to verify interesting closed-loop properties of heart and ICD.

Organization. Section 2 covers some preliminaries on hybrid systems. Sections 3 presents the heart model, and Sections 4-5 model the ICD. Sections 7 and 8 prove general results on STORMED systems that are used in the modeling: namely that a definable over-approximation of the flows such as that computed by SpaceEx preserves finiteness of the simulation, and that compositions of STORMED systems are STORMED.

Some material is relegated to an appendix, which is attached to the end of this paper for the reviewers' convenience. In the final version of this paper, the appendix will be moved online.

2. HYBRID SYSTEMS AND SIMULATIONS

This section presents fairly standard definitions on hybrid systems and their simulations [1]. It also defines STORMED hybrid systems, which admit finite bisimulations [23].

2.1 Transition and hybrid systems

Definition 2.1. *A* transition system $T = (Q, \Sigma, \to, Q_0)$ *consists of a set of states* Q*, a set of events* Σ *, a transition relation* $\to \subset Q \times \Sigma \times Q$*, a set of initial states* Q_0*. We write* $q \xrightarrow{\sigma} q'$ *to denote a transition element* $(q, q') \in \to$*. Given* $P \subset Q$*, we define* $Post_\sigma(P) := \{q' \mid \exists q \in P. q \xrightarrow{\sigma} q'\}$ *Given an equivalence relation* $\sim$ *on* Q*, the* quotient system $T/\sim$ *is* $T/\sim = (Q/\sim, \{*\}, \to_\sim, Q_0/\sim)$ *where* $[q] \xrightarrow{*}_\sim [q']$ *iff* $q \xrightarrow{\sigma} q'$ *for some* $\sigma \in \Sigma$*. Here* $[q]$ *is the equivalence class of* q *and* $Q/\sim$ *is the set of equivalence classes of* $\sim$*.*

Definition 2.2. *Given two transition systems* T_1 *and* T_2 *with the same state space* Q*, a* simulation *relation from* T_1 *to* T_2 *is a relation* $\mathcal{S} \subset Q \times Q$ *such that for all* $(q_1, q_2) \in \mathcal{S}$*, if* $q_1 \xrightarrow{\sigma}_1 q_1'$*, there exists a* $q_2' \in Q$ *s.t.* $q_2 \xrightarrow{\sigma}_2 q_2'$ *and* $(q_1', q_2') \in \mathcal{S}$*. A* bisimulation relation *between* T_1 *and* T_2 *is both a simulation relation from* T_1 *to* T_2 *and from* T_2 *to* T_1*.*

The bisimulation $\mathcal{B}$ is said to *respect* $\sim$ if $(q, q') \in \mathcal{B} \implies q \sim q'$. The following algorithm, if it terminates, yields a finite bisimulation for T that respects the given equivalence relation [1]. Moreover, it is the *coarsest* bisimulation (with respect to inclusion) that respects $\sim$. Given a set of atomic propositions AP, if $\sim$ is s.t. $q \sim q'$ iff both states satisfy exactly the same set of atomic propositions, then model checking CTL* properties can be done on the finite bisimulation instead of the possibly infinite T.

Algorithm 1 Computing a bismimulation respecting $\sim$

```
Require: Transition system $T = (Q, \Sigma, \rightarrow, Q_0)$, equivalence relation $\sim$.
  Set $\mathcal{S} = Q/\sim$
  while $\exists P, P' \in \mathcal{S}$ and $\sigma \in \Sigma$ s.t. $\emptyset \neq P' \cap Post_\sigma(P) \neq P'$ do
      Set $\mathcal{S} = \mathcal{S} \setminus \{P'\} \cup \{P' \cap Post_\sigma(P), P' \setminus Post_\sigma(P)\}$
  end while
  Return $\mathcal{S}$
```

Definition 2.3. *A* hybrid automaton *is a tuple*

$$\mathcal{H} = (X, L, H_0, \{f_\ell\}, Inv, E, \{R_{ij}\}, \{G_{ij}\})$$

where $X \subset \mathbb{R}^n$ is the continuous state space, $L \subset \mathbb{N}$ is a finite set of modes, $H_0 \subset H$ is an initial set, $\{f_\ell\}_{\ell \in L}$ determine the continuous evolutions with unique solutions, $Inv : L \rightarrow 2^X$ defines the invariants for every mode, $E \subset L^2$ is a set of discrete transitions, $\{G_{ij}\}_{(i,j)\in E}$ is a set of guard sets for the transitions, $\{R_{ij}\}_{(i,j)\in E}$ are edge-specific reset functions.
Set $H = L \times X$. Given $(\ell, x_0) \in H$, the flow *$\theta_\ell(;x_0) : \mathbb{R}_+ \rightarrow \mathbb{R}^n$ is the solution to the IVP $\dot{x}(t) = f_\ell(x(t))$, $x(0) = x_0$.*

The associated transition system is $T_\mathcal{H} = (H, E \cup \{\tau\}, \rightarrow, H_0)$ with $\rightarrow = (\bigcup_{e\in E} \xrightarrow{e}) \cup \xrightarrow{\tau}$ where $(i, x) \xrightarrow{e} (j, y)$ iff $e = (i, j), x \in G_{ij}, y = R_{ij}(x)$ and $(i, x) \xrightarrow{\tau} (j, y)$ iff $i = j$ and there exists a flow $\theta_i(\cdot; x)$ of $\mathcal{H}$ and $t \geq 0$ s.t. $\theta_i(t; x) = y$ and $\forall t' \leq t$, $\theta_i(t'; x) \in Inv(i)$. For a set $P \subset H$,$P_{|X}$ denotes its projection onto X, and $P_{|L}$ its projection onto L.

Definition 2.4. *[Reachability] Let $\mathcal{H}$ be a hybrid system with hybrid state space H, $I = [0, b) \subset [0, +\infty)$ be a (possibly unbounded) interval, $t \in I$, and $\epsilon > 0$. The ϵ*-approximate continuous reachability operator, *$\mathcal{R}^\epsilon_t : 2^H \rightarrow 2^H$ is given by*

$$\mathcal{R}^\epsilon_t(P) = \{(i, x) \in X | \exists x_0 \in P_{|X}, t \geq 0. ||\theta_i(t; x_0) - x|| \leq \epsilon\}$$

where $P = \{i\} \times W$, $W \subset Inv(i)$. Define also $\mathcal{R}^\epsilon_I(P) = \cup_{t\in I}\mathcal{R}^\epsilon_t(P)$. The (exact) discrete reachability operator *is:*

$$\mathcal{R}_d(P) \quad = \quad \cup_{j:(i,j)\in E} R_{ij}(P \cap G_{ij})$$

For a hybrid system, $Post_\sigma$ computes the forward reach sets, and is implemented by $\mathcal{R}^0_{[0,\infty)}$ and $\mathcal{R}_d$. Algorithm 1, applied to $T_\mathcal{H}$, implements the following iteration, in which $\mathcal{F}_t(\mathcal{P})$ is the coarsest bisimulation with respect to $\xrightarrow{\tau}$[1] respecting the partition $\mathcal{P}$, and $\mathcal{F}_d(\mathcal{P}) := \{(h_1, h_2) \mid (h_1 \xrightarrow{e} h'_1) \implies (\exists e' \in E, h'_2 .h_2 \xrightarrow{e'} h'_2 \wedge h'_1 \equiv_\mathcal{P} h'_2)\} \cap \mathcal{P}$ [23]:

$$W_0 = \mathcal{F}_t(Q/\sim), \quad \forall i \geq 0,\ W_{i+1} = \mathcal{F}_t(\mathcal{F}_d(W_i)) \qquad (1)$$

This iteration (equivalently, Alg. 1) does not necessarily terminate for hybrid systems because the reach set might intersect a given block of $Q/\sim$ an infinite number of times (see [11] for an example). The class of systems introduced in the next section has the property that Algorithm 1 does terminate for it and returns a finite $\mathcal{S}$, and therefore it admits finite bisimulations.

2.2 O-minimality and STORMED systems

We give a very brief introduction to o-minimal structures. A more detailed introduction can be found in [11], and an exposition of topology and o-minimality in [22]. We are interested in sets and functions in $\mathbb{R}^n$ that enjoy certain finiteness properties, called order-minimal sets (o-minimal). These are defined inside *structures* $\mathcal{A} = (\mathbb{R}, <, +, -, \cdot, \exp, \ldots)$. The subsets $Y \subset \mathbb{R}^n$ we are interested in are those that are *definable* using first-order formulas φ: $Y = \{(a_1, \ldots, a_n) \in \mathbb{R}^n \mid \varphi(a_1, \ldots, a_n)\}$. (First-order formulas use the boolean connectives and the quantifiers $\exists, \forall$). The atomic propositions from which the formulas are recursively built allow only the operations of the structure $\mathcal{A}$ on the real variables and constants, and the relations of $\mathcal{A}$ and equality. For example $2x - 3.6y < 3z$ and $x = y$ are valid atomic propositions of the structure $\mathcal{L}_\mathbb{R} = (\mathbb{R}, <, +, -, \cdot)$, while $cosh(x) < 3z$ is not because $cosh$ is not in the structure. These structures are already sufficient to describe a set of dynamics rich enough for our purposes and for various classes of linear systems.

Definition 2.5. *A theory of $(\mathbb{R}, \ldots)$ is* o-minimal *if the only definable subsets of $\mathbb{R}$ are finite unions of points and (possibly unbounded) intervals. A function $f : x \mapsto f(x)$ is o-minimal if its graph $\{(x, y) \mid y = f(x)\}$ is a definable set.*

We use the terms o-minimal and definable interchangeably, and they refer to the structure $\mathcal{L}_{\exp} = (\mathbb{R}, <, +, -, \cdot, \exp)$, which is known to be o-minimal. The dot product between $x, y \in \mathbb{R}^n$ is denoted $x \cdot y$, and $d(Y, S)$ is the minimum distance between sets Y and S.

Definition 2.6. *[23]. A* STORMED hybrid system *(SHS) Σ is a tuple $(\mathcal{H}, \mathcal{A}, \phi, b_-, b_+, d_{min}, \epsilon, \zeta)$ where $\mathcal{H}$ is a hybrid automaton, $\mathcal{A}$ is an o-minimal structure, $d_{min}, \zeta \in \mathbb{R}_+$, $b_-, b_+ \in \mathbb{R}$ and $\phi \in X^n$ such that:*
***(S)** The system is d_{min}-separable, meaning that for any $e = (\ell, \ell') \in E$ and $\ell'' \neq \ell'$,$d(R_e(G_{(\ell,\ell')}), G_{(\ell',\ell'')}) > d_{min}$* [2]
***(T)** The flows (i.e., the solutions of the ODEs) are Time-Independent with the Semi-Group property (TISG), meaning that for any $\ell \in L, x \in X$, the flow θ_ℓ starting at (ℓ, x) satisfies: 1) $\theta_\ell(0; x) = x$, 2) for every $t, t' \geq 0$, $\theta_\ell(t + t'; x) = \theta_\ell(t'; \theta_\ell(t; x))$*
***(O)** All the sets and functions of $\mathcal{H}$ are definable in the o-minimal structure $\mathcal{A}$*
***(RM)** The resets and flows are monotonic with respect to the same vector ϕ, meaning that*
1) (Flow monotonicity) for all $\ell \in L$, $x \in X$ and $t, \tau \geq 0$, $\phi \cdot (\theta_\ell(t + \tau; x) - \theta_\ell(t; x)) \geq \epsilon||\theta_\ell(t + \tau; x) - \theta_\ell(t; x)||$, and
2) (Reset monotonicity) for any edge $(\ell, \ell') \in E$ and any $x^-, x^+ \in X$ s.t. $x^+ = R_{\ell,\ell'}(x^-)$,

1. *if $\ell = \ell'$, then either $x^- = x^+$ or $\phi \cdot (x^+ - x^-) \geq \zeta$*
2. *if $\ell \neq \ell'$, then $\phi \cdot (x^+ - x^-) \geq \epsilon||x^+ - x^-||$*

***(ED)** Ends are Delimited: for all $e \in E$ we have $\phi \cdot x \in (b_-, b_+)$ for all $x \in G_e$*

Intuitively, the above conditions imply the trajectories of the system always move a minimum distance along ϕ whether flowing or jumping, which guarantees that no area of the state space will be visited infinitely often. This is at the

[1] I.e., $\mathcal{F}_t$ only considers the continuous transition relation. Namely, it is a bisimulation of $T^c_\mathcal{H} := (Q/\sim, \{*\}, \xrightarrow{\tau}, Q_0/\sim)$.

[2] We updated the definition of separability from [23] to accurately capture the requirement that if $\mathcal{H}$ flows, it flows a uniform minimum distance along ϕ. For this we need the starting point in the new mode, and any guard out of the mode, to be separated by at least d_{min}.

root of the finiteness properties of STORMED systems. The following result justifies the interest in STORMED systems: they admit finite bisimulations.

Theorem 2.1. *[23] Let $\mathcal{H}$ be a STORMED hybrid system, and let $\mathcal{P}$ be an o-minimal partition of its hybrid state space. Then $\mathcal{H}$ admits a finite bisimulation that respects $\mathcal{P}$.*

We need the following result in what follows.

Proposition 2.1. *If the state space X of a hybrid automaton $\mathcal{H}$ is bounded, then its guards have delimited ends.*

Proof. For all guard sets G and all $x \in G$, $||\phi \cdot x|| \leq ||\phi|| \cdot ||x|| \leq ||\phi||.\max\{||x||, x \in X\} < \infty$. □

3. HEART MODEL

For the verification of ICDs, we adopt the cellular automata (CA)-based heart model developed in [18],[19]. This model lies in-between high spatial fidelity but slow to compute PDE-based whole heart models [21], and low spatial fidelity but very fast-to-compute automata-based models [14]. PDE-based models are not currently amenable to formal verification, both theoretically and practically, and timed automata models can not simulate the electrograms needed for ICD verification. CA-based models were used in [12],[2] and [5]. This model also has the important advantage of forming the basis of software used to train physicians and electrophysiologists, and allows interactive simulation of surgical procedures like ablation [17].

In showing the various systems are STORMED, we partially depend on the specifics of the systems we model. The key observations are that, as will be seen in Section 5, i) the ICD will always reach a decision of VT or SVT in finite time, ii) at which point it flushes its variables so new values are computed for the next arrhythmia episode. So while the heart can beat indefinitely, for the purposes of ICD verification, there's a uniform upper bound on the length of time of any execution. Let $D \geq 0$ be this duration (D is on the order of 30sec depending on device settings). Moreover, the electrogram (EGM) voltage signal s has upper and lower bounds s_M and s_m. We also use the general results on STORMED systems that we establish in Sections 7-8.

3.1 Cellular automata model

The heart has two upper chambers called the *atria* and two lower chambers called the *ventricles* (Fig. 1) The synchronized contractions of the heart are driven by electrical activity. Under normal conditions, the SinoAtrial (SA) node (a tissue in the right atrium) spontaneously *depolarizes*, producing an electrical wave that propagates to the atria and then down to the ventricles (Fig.2) In this model, the myocardium (heart's muscle) is treated as a 2D surface (so it has no depth), and discretized into *cells*, which are simply regions of the myocardium (Fig. 2). Thus we end up with N^2 cells in a square N-by-N grid. A cell's voltage changes in reaction to current flow from neighboring cells, and in response to its own ion movements across the cell membrane. This results in an *Action Potential (AP).*

Fig. 3 shows how the AP is generated by a given cell [10]: in its quiescent mode (Phase 4), a cell (i, j) in the grid has a cross-membrane voltage $V(i, j, t)$ equal to $V_{min} < 0$. As it gathers charge, $V(i, j, t)$ increases until it exceeds a threshold voltage V_th. The voltage then experiences a very fast increase, called the upstroke, to a level $V_{max} > 0$, after which it decreases to a plateau. It stays at the plateau level for a certain amount of time **PD** then decreases linearly to below V_{th} (Phase 3 - ERP). Once below V_{th} it is said to be in the Relative Refractory Period (RRP). In RRP, the cell can be depolarized a second time, albeit at a higher threshold $V_{th,2}$, slower and to a lower plateau level $V_{max,2} < V_{max}$. Otherwise, when the voltage reaches V_{min} again, the cell enters the quiescent stage again. This model is suitable for both pacemaker and non-pacemaker cells, the main differences being in the duration of the plateau (virtually non-existent for pacemaker cells), and the duration of phases 0 and 4 (both are shorter for pacemaker cells).

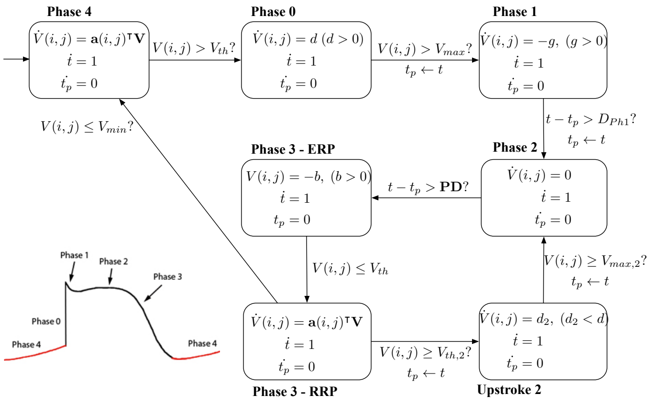


Figure 3: Hybrid model $\mathcal{H}_c$ of one cell of the heart model. AP figure from [8]. $V_{th,2} > V_{th}$**,** $V_{max,2} < V_{max}$

In Fig. 3, $V(i, j, t) \in \mathbb{R}$ denotes the voltage in cell (i, j) of the grid at time t, and vector $V = (V(1, 1), \ldots, V(N^2, N^2))^T$ in $\mathbb{R}^{N^2}$ groups the cross-membrane voltages of all cells in the heart. The whole heart model $\mathcal{H}_{CA}$ is the parallel composition of these N^2 single-cell models. The $(i, j)^{th}$ cell's voltage in Phase 4 depends on that of its neighbors and its own as follows [18]

$$\begin{aligned}\dot{V}(i,j,t) &= \frac{1}{R_h}[V(i-1,j,t) + V(i+1,j,t) - 2V(i,j,t)] \\ &\quad + \frac{1}{R_v}[V(i,j-1,t) + V(i,j+1,t) - 2V(i,j,t)] \\ &= a(i,j)^T V(t),\ a(i,j) \in \mathbb{R}^{N^2} \qquad (2)\end{aligned}$$

where R_h, R_v are conduction constants that can vary across the myocardium. Thus V evolves according to a linear ODE $\dot{V} = AV$ where A is the matrix whose rows are the $a(i, j)$. The two extra variables t and t_p are clocks.

ICDs observe the electrical activity through three channels (Fig. 1). Each signal is called an EGM signal. The signal read on a channel is the difference between two electrode potentials:

$$s(t) = \frac{1}{K}\sum_{i,j}\left(\frac{1}{||(i,j) - p_0||} - \frac{1}{||(i,j) - p_1||}\right)\dot{V}(i,j,t) \quad (3)$$

where p_0 and p_1 are the electrodes positions. This model was validated against real recordings taken in vitro [19].

Extensions. The APD restitution mechanism of heart cells, as modeled in [18], can be included in this model without changing its formal properties.

We now state and prove the main result of this section.

Theorem 3.1. *Let $\mathcal{H}_{CA}$ be the whole heart cellular automaton model obtained by parallel composition of N^2 models $\mathcal{H}_c$ with state vector $x = [V, t, t_p, s] \in \mathbb{R}^{N^2} \times \mathbb{R}^3$. Assume that all executions of the system have a duration of $D \geq 0$. Then $\mathcal{H}_{CA}$ is STORMED.*

Proof. We verify each property of STORMED. In this and all the proofs that follow, the approach is the same: (ED) holds by Lemma 2.1 because our state spaces are limited. After establishing properties (S), (T) and (O), we draw up the constraints on ϕ and ε imposed by reset and flow monotonicity (property (RM)). Then we argue that these constraints can be solved for ϕ and ε. Often there is more than one solution and we just point to one.

(S) Separability holds because $V_{min} < V_{th} < V_{th,2} < V_{max,2} < V_{max}$ and $PD > 0, D_{Ph_1} > 0$. For example, on transition **Phase 4** $\rightarrow$ **Phase 0**, $V(i,j) = V_{th}$, which is separated from the next guard $\{V(i,j) > V_{max}\}$ by $|V_{max} - V_{th}|$.
(T) All flows are linear or exponential and thus are TISG.
(O) The flows, resets and guard sets are all definable in $\mathcal{L}_{\exp}$. In particular the flow of $\dot{V} = AV$ is exponential with real exponent, and s is a sum of exponentials and linear terms.
(RM) We seek a vector $\phi = (\phi_V, \phi_t, \phi_p, \phi_s)^T \in \mathbb{R}^{N^2+3}$ such that resets and flows are monotonic along ϕ. Only transitions $p \rightarrow q \neq p$ are to be found in $\mathcal{H}_{CA}$, during which only t_p is reset. Always, $t_p^+ = t \geq t_p^-$, thus the reset is indeed monotonic as can be seen by choosing any $\varepsilon > 0$ and $\phi_p > \varepsilon$.

Monotonic flows: ϕ must also be such that in all modes:

$$\phi \cdot (\theta_\ell(t+\tau; x) - \theta_\ell(t; x)) \geq \varepsilon ||\theta_\ell(t+\tau; x) - \theta_\ell(t; x)||$$

Decomposing, we want

$$\begin{aligned} &\phi_V \cdot (V(t+\tau) - V(t)) + \phi_t \tau + \phi_p \cdot 0 \\ &\quad + \phi_s \cdot (s(x, t+\tau) - s(x,t)) \geq \varepsilon ||\theta_\ell(x, t+\tau) - \theta_\ell(x,t)|| \end{aligned}$$

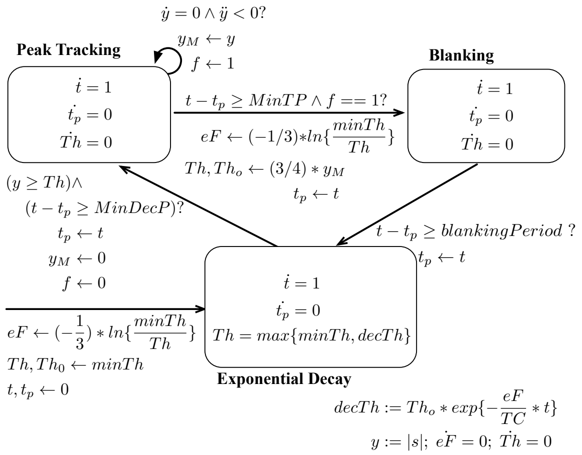
Now note that all flows have bounded derivatives in every bounded duration of flow and are thus Lipschitz. Let L_V be the Lipshitz constant of $V(t)$ and L_s that of $s(t)$. Then on the LHS of the above inequality we have $\phi_V \cdot (V(t+\tau) - V(t)) + \phi_s \cdot (s(t+\tau) - s(t)) \geq -\phi_V L_V \tau - \phi_s L_s \tau$. On the RHS we have $\varepsilon(L_V \tau + L_s \tau + \tau) \geq \varepsilon(||V(t+\tau) - V(t)|| + ||s(t+\tau) - s(t)|| + \tau) \geq \varepsilon(||\theta_\ell(x, t+\tau) - \theta_\ell(x,t)||)$ Thus (4) is satisfied if the stronger inequality

$$-\phi_V L_V \tau - \phi_s L_s \tau + \phi_t \tau \geq \varepsilon(L_V \tau + L_s \tau + \tau)$$

is satisfied. But this can be achieved by, for example, choosing $\phi_V = \phi_s = 0$ and $\phi_t \geq \varepsilon(L_V + L_s + 1)$.
(ED) Our system has bounded state spaces: V and s are voltages typically in the range $[-80, 60]$ mV and $t_p \leq t \leq D$. So (ED) holds by Lemma 2.1. □

4. ICD SENSING

Sensing is the process by which cardiac signals s measured through the leads of the ICD are converted to cardiac timing events. The ICD sensing algorithm is a threshold-based algorithm which declares events when the signal exceeds a dynamically-adjusted threshold Th.



$\dot{y} = 0 \wedge \ddot{y} < 0?$
$y_M \leftarrow y$
$f \leftarrow 1$
Peak Tracking
$\dot{t} = 1$
$\dot{t_p} = 0$
$\dot{Th} = 0$
$t - t_p \geq MinTP \wedge f == 1?$
$eF \leftarrow (-1/3) * ln\{\frac{minTh}{Th}\}$
$Th, Th_o \leftarrow (3/4) * y_M$
$t_p \leftarrow t$
Blanking
$\dot{t} = 1$
$\dot{t_p} = 0$
$\dot{Th} = 0$
$(y \geq Th) \wedge$
$(t - t_p \geq MinDecP)?$
$t_p \leftarrow t$
$y_M \leftarrow 0$
$f \leftarrow 0$
$t - t_p \geq blankingPeriod$?
$t_p \leftarrow t$
$eF \leftarrow (-\frac{1}{3}) * ln\{\frac{minTh}{Th}\}$
$Th, Th_0 \leftarrow minTh$
$t, t_p \leftarrow 0$
$\dot{t} = 1$
$\dot{t_p} = 0$
$Th = max\{minTh, decTh\}$
Exponential Decay
$decTh := Th_o * exp\{-\frac{eF}{TC} * t\}$
$y := |s|;\ \dot{eF} = 0;\ \dot{Th} = 0$

Figure 4: $\mathcal{H}_{Sense}$. States not shown in a mode have a 0 derivative, e.g., $\dot{eF} = 0$ in all modes.

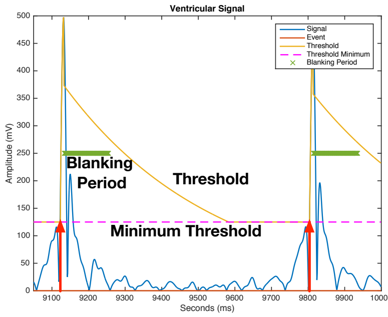


Figure 5: Example of dynamic threshold adjustment in ICD sensing algorithm. The shown signal is rectified.

Fig. 4 shows the model $\mathcal{H}_{Sense}$ of the sensing algorithm, and Fig. 5 illustrates its operation. The sensing takes place on the rectified EGM signal $y = |s|$. After an event is declared at the current threshold value ($y(t) \geq Th(t)$ in Fig. 4), the algorithm tracks the signal in order to measure the next peak's amplitude (mode Peak Tracking). For a duration $MinTP$ (min tracking period) the latest peak is saved in y_M. A variable f indicates that a peak was found. After a peak is found ($f == 1$) and after the end of the tracking period, the algorithm enters a fixed *Blanking Period*, during which additional events are ignored. On that transition, Th and Th_0 are set to 3/4 the current value of y_M and the exponential factor of decay is updated ($eF = (-1/3) * ln\frac{minTh}{TH}$). The algorithm then transitions to the Exponential Decay mode in which Th decays exponentially from Th_0 to a minimum level: $Th(t) = \max(minTh, Th_0 \cdot exp(-(eF/TC)t))$. The algorithm stays in the exponential decay mode for at least a sampling period of $MinDecP$. Correspondingly, there is a de facto Maximum Decay Period $MaxDecP$ after which the system transitions again to PeakTracking since the signal y is bound to exceed the minimum threshold $minTh$. Different manufacturers may use a step-wise decay instead of exponential, but the principle is the same.

Local peak detection is modeled via the $\dot{y} = 0 \wedge \ddot{y} < 0$ transition. While $y = |s|$ is non-differentiable at 0, the peak will occur away from 0, as shown in Fig. 5. The other states in Fig. 4 are t, t_p (clocks). $minTh$ and TC are constant parameters.

Theorem 4.1. *$\mathcal{H}_{Sense}$ is STORMED.*

Proof. **(S)** By definition, we only need to consider transitions between different modes to establish separability. For all such transitions, there is a minimum dwell time in the mode before taking the transition, namely $MinTP$ in PeakTracking, $BlankingPeriod$ in Blanking, and $MinDecP$ in mode ExponentialDecay. So the system is separable since there is a uniform minimum flow before jumping.
(T) Flows are either constant, (piece-wise) linear, or piece-wise linear and exponential (in the case of y and its derivatives) and therefore are TISG.
(O) All the flows, resets and guard sets are definable in $\mathcal{L}_{\text{exp}}$. (The absolute value and max functions can be broken down into boolean disjunctions of definable functions, and $t \mapsto \ln(t)$ is o-minimal by o-minimality of exp).
(RM) The state is $x = (t, t_p, y, y_M, f, Th, Th_0, eF) \in \mathbb{R}^8$, and let $\phi = (\phi_t, \phi_p, \phi_y, \phi_m, \phi_f, \phi_{Th}, \phi_0, \phi_{eF})$ be the corresponding ϕ vector. Recall that the EGM voltage s, and so $y = |s|$, is upper-bounded by V_M.
ExponentialDecay → PeakTracking. Only t_p, y_M and f are modified, so monotonicity produces the constraint $\phi_p(t-t_p)+\phi_m(0-y_M)+\phi_f(0-1) \overset{Want}{\geq} \varepsilon(|t-t_p|+|y_M|+1)$. We require the stronger constraint to hold:

$$\phi_t MinDecP - \phi_m V_M - \phi_f \overset{Want}{\geq} \varepsilon(MaxDecP + V_M + 1)$$

PeakTracking → PeakTracking. Only y_M and f are reset. Algebraic manipulation yields $-2V_M\phi_m + \phi_f \overset{Want}{\geq} \zeta$
PeakTracking → Blanking. t_p, eF, Th and Th_0 are reset, so we get

$$\begin{aligned} &\phi_p(t-t_p) + \phi_{eF}(-(1/3)\ln(minTh/Th) - eF) \\ &+\phi_{Th}(3y_M/4 - Th) + \phi_0(3y_M/4 - Th_0) \\ &\geq \varepsilon(|t-t_p| + |-\frac{1}{3}\ln(\frac{minTh}{Th}) - eF| \\ &+|\frac{3y_M}{4} - Th| + |\frac{3y_M}{4} - Th_0|) \end{aligned}$$

Th is lower-bounded by $minTh$ at all times, and it is naturally upper-bounded by V_M as the threshold should never exceed the largest possible attainable voltage. By the same token, $0 \leq eF \leq (1/3)\ln(V_M/minTh)$. Then we want the stronger inequality

$$\begin{aligned} \phi_p MinTP \quad &+ \quad \phi_{eF}(0 - (1/3)\ln(V_M/minTh) \\ &+ \quad \phi_{Th}(-V_M) + \phi_0(-V_M) \\ &\geq \quad \varepsilon(MaxTP + |\frac{1}{3}\ln(\frac{V_M}{Th})| + |V_M| + |V_M|) \end{aligned}$$

Blanking → ExponentialDecay. Only t_p is reset and therefore we want, $\phi_p(t-t_p) \geq \varepsilon(|t-t_p|)$, thus the transition yields $\phi_p \geq \varepsilon$.

The above equations can be simultaneously satisfied. The simplest thing would be to set all ϕ terms that appear above to 0 except for ϕ_t, ϕ_p which are calculated accordingly.

The flows can be shown to be monotonic along the same ϕ and with the same ε. For example, in mode ExponentialDecay, only t, y and Th flow. Making use of the V_M bound on y, we get the constraint $\phi_t\tau - 2V_M\phi_y + \phi_{Th}(Th(t+\tau) - Th(t)) \geq \varepsilon(\tau + 2V_M + |Th(t+\tau) - Th(t)|)$, which yields $\phi_t \geq \varepsilon$, $\phi_y \leq -\varepsilon$ and $\phi_{Th} \geq \varepsilon$. Similarly for the rest. □

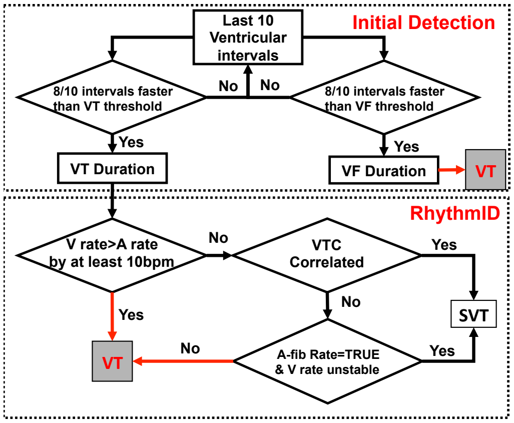


Figure 6: Boston Scientific's detection algorithm

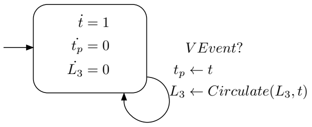


Figure 7: Three Consecutive Fast Intervals $\mathcal{H}_{TCFI}$

5. ARRHYTHMIA DETECTION

Disturbances of the heart's normal rhythm are known as *arrhythmias*. *Ventricular Tachycardia (VT)* is an example of an arrhythmia originating in the ventricles, in which the ventricles spontaneously beat at a very high rate. If the VT is sustained, or degenerates into Ventricular Fibrillation (VF), it is fatal within seconds. An abnormally fast heart rate that originates in the atria is referred to as a *SupraVentricular Tachycardia (SVT)*. This is a diseased but non-fatal condition. In what follows, we will refer to sustained VT and VF together as VT. *The ICD's main task is to discriminate VT from SVT and deliver therapy to the former.*

Most VT/SVT detection algorithms found in ICDs today are composed of individual *discriminators*. A discriminator is a software function whose task is to decide whether the current arrhythmia is SVT or VT. No one discriminator can fully distinguish between SVT and VT. Thus a detection algorithm is often a decision tree built using a number of discriminators *running in parallel*. The detection algorithm of Boston Scientific is shown in Fig. 6 [3]. We have modeled each discriminator in this detection algorithm as a STORMED hybrid system. The algorithm itself is then a hybrid system. **The ICD system is thus $\mathcal{H}_{\textbf{ICD}} = \mathcal{H}_{\textbf{Sense}}||\mathcal{H}_{\textbf{Detection-Algo}}$ where $\mathcal{H}_{\textbf{Detection-Algo}}$ is the parallel composition of the discriminator systems**. In what follows, we present three of these discriminators we modeled, which are found in most ICDs and model them as hybrid systems, and prove they are STORMED.

5.1 Three Consecutive Fast Intervals

Our first module simply detects whether three consecutive fast intervals have occurred, where 'fast' means the interval length, measured between 2 consecutive peaks on the EGM signal, is shorter than some pre-set amount. See Fig. 7. It has one running clock t, and a clock t_p that keeps track of the value of the last discrete jump. We will use this arrangement in all our models: it avoids resetting the clocks which preserves Reset Monotonicity. The vector L_3 is three-dimensional, and stores the values of the last three

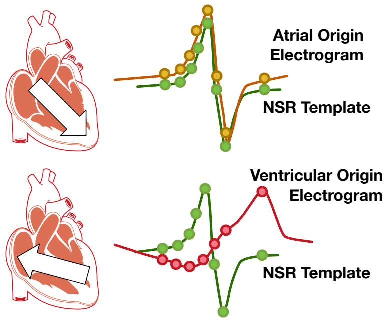


Figure 8: EGMs of different origin have different morphologies. The correlation of an EGM with respect to a stored EGM template is used to determine the origin.

intervals. The event VEvent? is shorthand for the transition $y(t) \geq Th$ being taken by the $\mathcal{H}_{Sense}$ automaton. In other words, it indicates a ventricular event. Then L_3 gets reset to $L_3^+ = (z_1, z_2, z_3)^+ := \text{Circulate}(L_3, t - t_p)$ where

$$L_3^+ = \begin{pmatrix} z_2 \\ z_3 \\ t - t_p \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} L_3 + \begin{pmatrix} 0 \\ 0 \\ t - t_p \end{pmatrix} \tag{4}$$

Lemma 5.1. *$\mathcal{H}_{TCFI}$ is STORMED.*

Proof. We show that the reset are monotonic - the other properties are easily checked. For reset monotonicity, we invoke the fact that there is a minimum beat-to-beat separation: heartbeats can't follow one another with vanishingly small delays. In other words, there exists $m > 0$ such that $t - t_p^- > m$. Similarly, there's a maximum delay between two heartbeats, call it B. Now, we seek a vector $\phi \in \mathbb{R}^5$ s.t.

$$\phi \cdot \begin{pmatrix} t - t \\ t - t_p \\ L_3^+ - L_3 \end{pmatrix} = \phi_p(t - t_p) + \phi_{L_3} \cdot \underbrace{\begin{pmatrix} z_2 - z_1 \\ z_3 - z_2 \\ t - t_p - z_3 \end{pmatrix}}_{\delta} \overset{Want}{\geq} \zeta > 0 \tag{5}$$

Now $|\delta|$ is upper bounded by $\sqrt{3 \cdot (2B)^2}$ since each element is the difference of intervals shorter than B. Also, $t - t_p^- > m > 0$. So choose $\phi_{L_3} = (\phi_{z,1}, \phi_{z,2}, \phi_{z,3}) > 0$ elementwise. (5) is satisfied if the following stronger inequality is satisfied, which can be achieved by an appropriate choice of $\phi_{z,i}$: $\phi_p m \geq \zeta + \sqrt{12B^2} \sum_1^3 \phi_{z,i}$ □

5.2 Vector Timing Correlation

It has been clinically observed that a depolarization wave originating in the ventricles (as produced during VT for example) will in general produce a different EGM morphology than a wave originating in the atria (as produced during SVT) [3]. See Fig. 8. A morphology discriminator measures the correlation between the morphology of the current EGM and that of a stored *template* EGM acquired during normal sinus rhythm. If the correlation is above a pre-set threshold for a minimum number of beats, then this is an indication that the current arrhythmia is supraventricular in origin. Otherwise, it might be of ventricular origin.

Boston Scientific's implementation of a morphology discriminator is called Vector and Timing Correlation (VTC). VTC first samples 8 *fiducial* points $s_i, i = 1, \ldots, 8$ on the current EGM s at pre-defined time instants. Let $s_{m,i}$ be the corresponding points on the template EGM. The correlation is

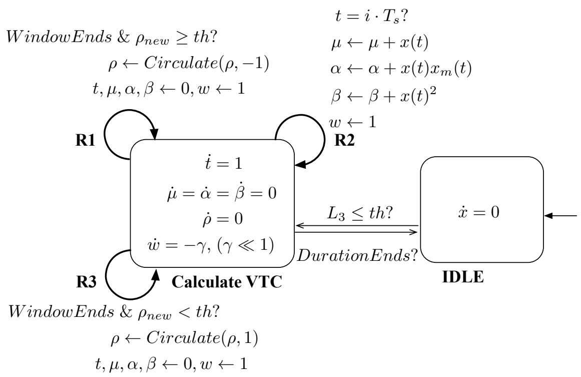

$WindowEnds$ & $\rho_{new} \geq th?$
$\rho \leftarrow Circulate(\rho, -1)$
$t, \mu, \alpha, \beta \leftarrow 0, w \leftarrow 1$
$t = i \cdot T_s?$
$\mu \leftarrow \mu + x(t)$
$\alpha \leftarrow \alpha + x(t)x_m(t)$
$\beta \leftarrow \beta + x(t)^2$
$w \leftarrow 1$
R1
R2
$\dot{t} = 1$
$\dot{\mu} = \dot{\alpha} = \dot{\beta} = 0$
$\dot{\rho} = 0$
$\dot{w} = -\gamma, (\gamma \ll 1)$
$L_3 \leq th?$
$DurationEnds?$
$\dot{x} = 0$
R3
Calculate VTC
IDLE
$WindowEnds$ & $\rho_{new} < th?$
$\rho \leftarrow Circulate(\rho, 1)$
$t, \mu, \alpha, \beta \leftarrow 0, w \leftarrow 1$

Figure 9: VTC calculation. iT_s is the sampling time.

then calculated as [3] $\rho_{new} = \frac{(8\sum s_i s_{m,i} - (\sum s_i)(\sum s_{m,i}))^2}{(8\sum s_i^2 - (\sum s_i)^2)(8\sum s_{m,i}^2 - (\sum s_{m,i})^2)}$ Note that s_m is a constant for the purposes of this calculation: it does not change during an execution of VTC. If 3 out of the last 10 calculated correlation values exceed the threshold, then SVT is decided and therapy is withheld.

The system of Fig. 9 implements the VTC discriminator. As before, t is a local clock. μ accumulates the values of the current EGM, α accumulates the product $s_i s_{m_i}$, β accumulates s_i^2. State w is an auxiliary state we need to establish the STORMED property. $\vec{\nu}$ is a 10D binary vector: $\vec{\nu}(i) = -1$ if the i^{th} correlation value fell below the threshold, and is $+1$ otherwise. L_3 is the state of $\mathcal{H}_{TCFI}$: the guard condition $L_3 \leq th$ indicates that all its entries have values less than the tachycardia threshold, which is when $\mathcal{H}_{VTC}$ starts computing. *BeatEnds* indicates the 'end' of an EGM, measured as a window around the peak sensed by $\mathcal{H}_{Sense}$.

Lemma 5.2. *$\mathcal{H}_{VTC}$ is STORMED.*

Proof. **S**eparability obtains by observing that a uniform minimum time passes between beats and between samples. **T**ISG is immediate. **O**-minimality is established by observing that all sets and functions are definable in $\mathcal{L}_{\exp}$. **ED** holds because the state space is bounded. We now show monotonicity. The state of the system is $x = (t, \mu, \alpha, \beta, \vec{\nu}, w)^T \in \mathbb{R}^{4+10+1}$ Let $\phi = (\phi_c, \phi_\mu, \phi_\alpha, \phi_\beta, \phi_1, \ldots, \phi_{10}, \phi_w)^T \in \mathbb{R}^{15}$ be the corresponding vector. For flows in mode CalculateVTC, we seek a ϕ and $\varepsilon > 0$ such that $\phi \cdot (t + \tau - t, \mathbf{0}, -\gamma(t + \tau) + \gamma t) = \phi_c \tau + \phi_w(-\gamma\tau) \geq \varepsilon\sqrt{\tau^2 + \gamma^2\tau^2}$, which is equivalent to $\boxed{\phi_c - \phi_w\gamma \geq \varepsilon\sqrt{1 + \gamma^2}}$. Reset monotonicity provides three more constraints on ϕ and ε:

$$\begin{aligned}
\textbf{(R1)} \quad & \phi \cdot (-t, -\mu, -\alpha, -\beta, \nu_2 - \nu_1, \nu_3 - \nu_2, \ldots, -1 - \nu_{10}) \\
= \quad & -\phi_c t - \phi_\mu \mu - \phi_\alpha \alpha - \phi_\beta \beta + \sum_{i=1}^{10} \phi_i(\nu_{i+1} - \nu_i) \\
& +\phi_w(1 - w) \overset{Want}{\geq} \zeta \\
\textbf{(R2)} \quad & \phi \cdot (t - t, s, s \cdot s_m, s^2, \mathbf{0}, 1 - w) \\
= \quad & \phi_\mu s + \phi_\alpha s s_m + \phi_\beta s^2 + \phi_w(1 - w) \overset{Want}{\geq} \zeta > 0 \\
\textbf{(R3)} \quad & -\phi_c t - \phi_\mu \mu - \phi_\alpha \alpha - \phi_\beta \beta + \sum_{i=1}^{10} \phi_i(\nu_{i+1} - \nu_i) \\
& +\phi_w(1 - w) \overset{Want}{\geq} \zeta
\end{aligned}$$

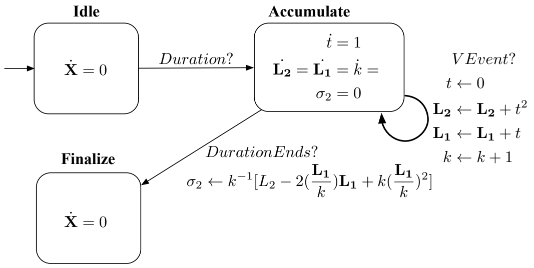

Idle
$\dot{\mathbf{X}} = 0$
Duration?
Accumulate
$\dot{t} = 1$
$\dot{\mathbf{L_2}} = \dot{\mathbf{L_1}} = \dot{k} =$
$\sigma_2 = 0$
VEvent?
$t \leftarrow 0$
$\mathbf{L_2} \leftarrow \mathbf{L_2} + t^2$
$\mathbf{L_1} \leftarrow \mathbf{L_1} + t$
$k \leftarrow k + 1$
DurationEnds?
$\sigma_2 \leftarrow k^{-1}[L_2 - 2(\frac{\mathbf{L_1}}{k})\mathbf{L_1} + k(\frac{\mathbf{L_1}}{k})^2]$
Finalize
$\dot{\mathbf{X}} = 0$

Figure 10: Stability discriminator.

where $\nu_{11} := -1$ in **R1** and $\nu_{11} := 1$ in **R3**. Combine **R1** and **R3** by choosing $\phi_1 = \ldots = \phi_{10} = \phi_\mu = \phi_\alpha = \phi_\beta = 0$:

$$(\mathbf{R1}, \mathbf{3}) \ -\phi_c t + \phi_w(1 - w) \geq \zeta$$

$$(\mathbf{R2}) \ \phi_w(1 - w) \geq \zeta$$

Now note that when a reset occurs, $0 < w \leq 1 - \gamma T_s := w_m$ where T_s is the smallest sampling period, and that $t \leq 10B$, $B =$ the maximum peak-to-peak interval, so $(\mathbf{R2})$, $(\mathbf{R1}, \mathbf{3})$ can be jointly satisfied if $\boxed{-\phi_c 10B + \phi_w(1 - w_m) \geq \zeta}$. The 2 boxed equations can be jointly satisfied. □

5.3 Stability discrimination

Stability refers to the variability of the peak-to-peak cycle length. A rhythm with large variability (above a pre-defined threshold) is said to be *unstable*, and is called stable otherwise. The Stability discriminator is used to distinguish between atrial fibrillation, which is usually unstable, and VT, which is usually stable.

The Stability discriminator shown in Fig. 10 simply calculates the variance of the cycle length over a fixed period called a Duration (measured in seconds). Let $DL \geq 0$ be the Duration length. The event $DurationEnds?$ indicates a transition of a simple system that measures the lapse of one Duration (not shown here). State t is a clock, L_1 accumulates the sum of interval lengths (and will be used to compute the average length), L_2 accumulates the squares of interval lengths, and κ is a counter that counts the number of accumulated beats. σ_2 is assigned the value of the variance given by $\frac{1}{\kappa}[L_2 - 2L_1/\kappa + \kappa(L_1/\kappa)^2]$

Lemma 5.3. *$\mathcal{H}_{Stab}$ is STORMED.*

The proof is in the Appendix.

Now that each system was shown to be STORMED, it remains to establish that their parallel composition is STORMED. This result does not hold in general - Thm. 7.1 gives conditions under which parallel composition respects the STORMED property. Intuitively, we require that whenever a sub-collection of the systems jumps, the remaining systems that did not jump are separated from all of their respective guards by a uniform distance. This is a requirement that can be shown to hold for our systems by modeling various minimal delays in the systems' operation. We may now state:

Theorem 5.1. *Consider the collection of systems $\mathcal{H}_{CA}$, $\mathcal{H}_{ICD} = \mathcal{H}_{Sense}||\mathcal{H}_{Detection-Algo}$ where the latter is the parallel composition of the discriminator systems. This collection satisfies the hypotheses of Thm. 7.1 (Section 7) and therefore the parallel system $\mathcal{H}_{CA}||\mathcal{H}_{ICD}$ is STORMED and has a finite bisimulation.*

6. PROPERTIES OF INTEREST

The finite simulation we obtain by running (the approximate version of) Alg. 1 abstracts away the duration of continuous transitions $\xrightarrow{\tau}$, so that only time-unbounded properties (like LTL) can be verified on the abstraction. However, every component of $\mathcal{H}_{ICD}$ has a local clock in its state vector. Thus these clocks can be used to express interesting time-bounded properties of $\mathcal{H}_{ICD}||\mathcal{H}_{CA}$.

For example, to expresses that a Sustained VT event should be followed by a VT determination within 30sec, we write:

$$\varphi_{Th} := \varphi_{VT} \implies \varphi_{VT}\mathcal{U}_{[0,30]}\mathcal{H}_{ICD}.Mode = VT \quad (6)$$

The VT decision ($\mathcal{H}_{ICD}.Mode = VT$) can be reached by one of three paths of execution (see Fig. 6): For example, path P_1 goes from the root to "8/10 faster" on the right and ends in VT. Along each path, the component automata have local clocks that keep track of how long they are running in this execution. Therefore, the total execution time of all automata on a given path must be less than 30sec. So the time constraint may now be expressed as the disjunction $\vee_{P \in \{P_1, P_2, P_3\}} \sum_{c \in P} c \leq 30$. The formula can be re-written

$$\varphi_{VT} \implies \varphi_{VT}\mathcal{U}\vee_{k=1,2,3}(\mathcal{H}_{ICD}.Mode = VT_k \wedge \sum_{c \in P_k} c \leq 30)$$

where VT_k is the VT decision reached along the k^{th} path.

7. COMPOSING STORMED SYSTEMS

The results in this section and the next apply to STORMED systems in general, including those with time-unbounded operation. We write $[m] = \{1, \ldots, m\}$.

We show that the parallel composition of SHS is still a SHS. Recall that $\theta_\ell(t; x)$ is the flow starting at (ℓ, x). Given hybrid systems $\mathcal{H}_1, \ldots, \mathcal{H}_m$, their parallel composition $\mathcal{H} = \mathcal{H}_1|| \ldots ||\mathcal{H}_m$ is defined in the usual way: $\mathcal{H}.X = \Pi_i X_i$, $\mathcal{H}.L = \Pi_i L_i$, $\mathcal{H}.H_0 = \Pi_i H_{0_i}$, $Inv(\ell) = \Pi_i Inv_i(\ell_i)$, $\theta_\ell(x, t) = [\theta^1_{\ell_1}(x_1, t)(t), \ldots, \theta^m_{\ell_m}(x_m, t)(t)]^T$. The system jumps if any of its subsystems jumps, so its guard sets are of the form $D_1 \times \ldots \times D_m$ where for at least one i, D_i is a guard of $\mathcal{H}_i$, and for the rest $D_j = X_j$. When a guard of a subsystem is satisfied, the state of that subsystem is reset according to its reset map. Formally, the guards are made disjoint to avoid non-determinism.

In general $\mathcal{H}$ is not separable: indeed for any candidate value of d_{min}, one could find a transition (i, j) of $\mathcal{H}$ due to, say, a jump of $\mathcal{H}_1$, s.t. at that moment x_2 is closer than d_{min} to its own guard. This causes $\mathcal{H}$ to jump $j \to k$ without having traveled the requisite minimum distance, thus violating the separability of $R_{ij}(G_{ij})$ and G_{jk}. Therefore we need to impose an extra condition on minimum separability *across* sub-systems. This extra condition is satisfied by $\mathcal{H}_{ICD}||\mathcal{H}_{CA}$ as can be seen by inspection.

Theorem 7.1. *Let $\Sigma_i = (\mathcal{H}_i, \mathcal{A}, \phi_i, b_i^-, b_i^+, d_{min,i}, \varepsilon_i, \zeta_i)$, $i = 1, \ldots, m$ be deterministic SHS defined using the same underlying o-minimal structure, and where each state space X_i is bounded by B_{X_i}. Assume that the following **Collection Separability** condition holds: for all $i, j \leq m$ there exists $d^{ij}_{min} > 0$ s.t. $x_i \in G^i_e \implies d(x_j, G^j_{e'})) > d^{ij}_{min}$ for all $e' \in E_i$ where G^k_e is a guard of Σ_k on edge e and E_k is the edge set of Σ_k.*

Define parallel composition $\Sigma = (\mathcal{H}, \mathcal{A}, \phi, b^-, b^+, d_{min}, \varepsilon, \zeta)$ *where* $\mathcal{H} = \mathcal{H}_1 || \dots || \mathcal{H}_m$, $\phi = (\phi_1, \dots, \phi_m)^T \in \mathbb{R}^{mn}$, $b_i^- = \inf_{x \in X} \phi \cdot x$, $b_i^+ = \sup_{x \in X} \phi \cdot x$, $\varepsilon = \min(\min_i \varepsilon_i, \min_i \frac{\zeta_i}{B_{X_i}})$,

$$d_{min} = \min_{I \subset [m]} (\min_{i \in I} d^i_{min}, \min_{i \in I, j \in [m] \setminus I} d^{ij}_{min})$$

$\zeta = \min_i \zeta_i$. *Then* Σ *is STORMED.*

Proof. **(S)** In $\mathcal{H}$, let $y = (y_1, \dots, y_m) = R_e((x_1, \dots, x_m))$ and assume without loss of generality that it was $\mathcal{H}_1$ that caused the jump. Thus $y_j = x_j, j > 1$. Write $e = (\ell, \ell')$. By hypothesis $d(y_j, G^j_{e_j}) > d^{1j}_{min}$ for all $j > 1, e_j \in E_j$, and by separability of $\mathcal{H}_1$ $d(y_1, G^1_{e_1}) > d^1_{min}$ so $d(y, G_{\ell', \ell''}) > \min(d^1_{min}, \min_{j>1} d^{1j}_{min})$ for any guard leading out of ℓ', and we have separability. The argument can be repeated for any set $I \subset [m]$ of systems jumping simultaneously.
(T): let $\ell = (\ell_1, \dots, \ell_m)$ and $x = (x_1, \dots, x_m)$. The $\widehat{\mathcal{H}}$ flow $\widehat{\theta}_\ell(t; \hat{x}) = (\ell(t), \theta_\ell(t; x))$ is TISG because the component flows $\theta^i_{\ell_i}(t; x_i)$ and $\ell(t) \equiv \ell$ are TISG.
(O) The cartesian product of definable sets is definable, so the system $\widehat{\mathcal{H}}$ is o-minimal.
(RM) First we show that resets of $\mathcal{H}$ are monotonic, then that the resets of $\widehat{\mathcal{H}}$ are monotonic. Let $p, q \in L$ be two modes of $\mathcal{H}$, $p \neq q$.

Case 1: $\mathcal{H}$ jumps $p \to p$. So any subsystem $\mathcal{H}_i$ either jumped $p_i \to p_i$ or didn't jump at all. If $x^+ = x^-$, then (RM) is satisfied. Else, define $\phi := (\phi_1, \dots, \phi_m) \in \mathbb{R}^{n \cdot m}$, where ϕ_i is the ϕ vector of system $\mathcal{H}_i$. Then $\phi \cdot (x^+ - x^-) = \sum_{i \in K} \phi_i \cdot (x_i^+ - x_i^-)$, where $K \subset [m]$ is the set of indices of sub-systems that jumped with $x_i^- \neq x_i^+$. Note that K depends on x^-, x^+. For all x^-, x^+ pairs (and so for all K) $\sum_{i \in K} \zeta_i \geq \min_{i \in [m]} \zeta_i := \zeta > 0$. So by (RM) for each $\mathcal{H}_i$,

$$\phi \cdot (x^+ - x^-) \geq \sum_{i \in K} \phi_i \cdot (x_i^+ - x_i^-) \geq \sum_{i \in K} \zeta_i \geq \zeta > 0$$

Thus (RM) is satisfied.

Case 2: $\mathcal{H}$ jumps $p \to q$. At least one syb-system $\mathcal{H}_i$ jumped $p_i \to q_i \neq p_i$. Then $\phi \cdot (x^+ - x^-) = \sum_{i \in [m]} \phi_i \cdot (x_i^+ - x_i^-) = \sum_{i \in K} \phi_i \cdot (x_i^+ - x_i^-)$, where $K = K_= \cup K_{\neq} \subset [m]$ and $K_=$ is the index set of subsystems that jumped $p_i \to p_i$ with $x_i^+ \neq x_i^-$, and $K_{\neq}$ is the index set of subsystems that jumped $p_i \to q_i \neq p_i$ with $x_i^+ \neq x_i^-$. Subsystems that didn't jump or jumped without changing their state don't contribute to the sum. Note that $K_=, K_{\neq}$ depend on x^-, x^+. So we have $\phi \cdot (x^+ - x^-) \geq \sum_{i \in K_{\neq}} \varepsilon_i ||x_i^+ - x_i^-|| + \sum_{i \in K_=} \zeta_i$.

For all X_i, $||x_i^+ - x_i^-|| \leq B_{X_i}$ for all $x_i^-, x_i^+ \in X_i$. Therefore $\zeta_i \frac{||x_i^+ - x_i^-||}{B_{X_i}} \leq \zeta_i$ for all $i \in K$. So

$$\begin{aligned} & \sum_{i \in K_{\neq}} (\min_{i \in [m]} \varepsilon_i) ||x_i^+ - x_i^-|| + \sum_{i \in K_=} \frac{\zeta_i}{B_{X_i}} ||x_i^+ - x_i^-|| \\ \geq & \sum_{i \in K_{\neq}} (\min_{i \in [m]} \varepsilon_i) ||x_i^+ - x_i^-|| + \sum_{i \in K_=} (\min_{i \in [m]} \frac{\zeta_i}{B_{X_i}}) ||x_i^+ - x_i^-|| \end{aligned}$$

Let $\varepsilon := \min(\min_i \varepsilon_i, \min_i \frac{\zeta_i}{B_{X_i}})$. Then

$$\phi \cdot (x^+ - x^-) \geq \sum_{i \in K} \varepsilon ||x_i^+ - x_i^-|| \geq \varepsilon ||x^+ - x^-||$$

So $\mathcal{H}$ has monotonic resets.

What about $\widehat{\mathcal{H}}$? Consider again the case where $\mathcal{H}$ jumps $p \to q \neq p$, the other case being trivial. Fix an arbitrary $\phi_d \leq -\varepsilon$. Let $\hat{x} = (x, \ell)$ be the state of $\widehat{\mathcal{H}}$, and let $\hat{\phi} = (\phi, \phi_d)$ with $\phi = (\phi_1, \dots, \phi_m)$ as defined above. Then $\hat{\phi} \cdot (\hat{x}^+ - \hat{x}^-) = \phi \cdot (x^+ - x^-) + \phi_d \cdot (q - p) \geq \varepsilon ||x_i^+ - x_i^-|| + \phi_d (1 - |L|) \geq \varepsilon ||x_i^+ - x_i^-|| + \varepsilon(|L| - 1) \geq \varepsilon ||x_i^+ - x_i^-|| + \varepsilon |q - p|$ and the resets of $\widehat{\mathcal{H}}$ are monotonic.

The flows of $\widehat{\mathcal{H}}$ are also monotonic along $\hat{\phi} = (\phi, \phi_d)$. Indeed for any $q \in L$, $\hat{\phi} \cdot (\hat{\theta}_q(t + \tau; x) - \hat{\theta}_q(t; x)) = \phi \cdot (\theta_q(t + \tau; x) - \theta_q(t; x)) + \phi_d \cdot (q - q) = \sum_{i=1}^m \phi_i \cdot (\theta^i_{q_i}(t + \tau; x_i) - \theta^i_{q_i}(t; x_i)) \geq \varepsilon_i ||(\theta^i_{q_i}(t + \tau; x_i) - \theta^i_{q_i}(t; x_i))|| \geq \varepsilon ||(\theta_q(t + \tau; x) - \theta_q(t; x))|| = \varepsilon ||\hat{\theta}_q(t + \tau; x) - \hat{\theta}_q(t; x)||$

(ED) By Prop. 2.1. □

8. FINITE SIMULATION FOR STORMED SYSTEMS

In general it is not possible to compute the reach sets required in Alg. 1 exactly unless the underlying o-minimal theory is decidable. The $\mathcal{H}_{ICD} || \mathcal{H}_{CA}$ closed loop is definable in $\mathcal{L}_{\exp}$, and the latter is not known to be decidable. The authors in [15] proposed approximating the flows and resets by polynomial flows and resets in the decidable theory $\mathcal{L}_{\mathbb{R}}$. However, the approximation process is typically iterative and requires manual intervention, or is restricted to subclasses of STORMED systems [15].

Here we show that if an approximate reachability tool with definable over-approximations is available for the continuous dynamics, it can be used in Algo 1 (instead of exact reachability) to yield a finite simulation (rather than a bisimulation). Intuitively, the additional intersections of approximate reach sets with blocks of $Q/\sim$ do not destroy finiteness of the procedure. Since we only have a simulation, counter-examples on the abstraction should be validated in a CEGAR-like fashion.

Lemma 8.1. *Let* $\Sigma = (\mathcal{H}, \dots)$ *be a SHS and* $\sim$ *and equivalence relation on* X. *For any mode* ℓ *of* $\mathcal{H}$, *its dynamical sub-system* $\mathcal{D}$ *with state space* $X = \mathcal{H}.X$ *and flow* θ_ℓ *admits a finite simulation* $\mathcal{S}_\ell$ *that respects* $\sim$, *returned by Alg. 1.*

The proof is in the Appendix. Let $\mathcal{F}_t^\epsilon(\mathcal{P}) := \cap_\ell \mathcal{S}_{\ell \in L}$ where $\mathcal{P} = X/\sim$. $\mathcal{F}_t^\varepsilon$ refines all the $\mathcal{S}_\ell$'s, and it is a finite simulation of $\mathcal{H}$ by itself w.r.t. the continuous transition $\xrightarrow{\tau}$. It is clear that $\mathcal{F}_t^\epsilon(\cdot)$ is idempotent: $\mathcal{F}_t^\epsilon(\mathcal{F}_t^\epsilon(\mathcal{P})) = \mathcal{F}_t^\epsilon(\mathcal{P})$

Theorem 8.1. *Let* $\mathcal{H}$ *be a STORMED hybrid system, and* $\mathcal{P}$ *be a finite definable partition of its state space. Define*

$$W_0 = \mathcal{F}_t^\epsilon(\mathcal{P}), \quad \forall i \geq 0, W_{i+1} = \mathcal{F}_t^\epsilon(\mathcal{F}_d(W_i)) \qquad (7)$$

Then there exists $U \in \mathbb{N}$ *s.t.* $W_{U+1} = W_U$ *and* $\mathcal{F}_t^\epsilon(W_U)$ *is a simulation of* $\mathcal{H}$ *by itself.*

Proof. By Lemma 10 of [23] there exists a uniform bound U on the number of discrete transitions of any execution of the STORMED system $\mathcal{H}$, so $\mathcal{F}_d(W_k) = W_k$ for all $k \geq U$. Moreover $W_{U+1} = \mathcal{F}_t^\epsilon(\mathcal{F}_d(W_U)) = \mathcal{F}_t^\epsilon(W_U)$ and $W_{U+2} = \mathcal{F}_t^\epsilon(\mathcal{F}_d(W_{U+1})) = \mathcal{F}_t^\epsilon(\mathcal{F}_t(W_U)) = \mathcal{F}_t^\epsilon(W_U) = W_{U+1}$, so the iterations reach a fixed point. The fact that $\mathcal{F}_t^\epsilon(W_U)$ is a simulation then yields the desired result. □

8.1 Example: SpaceEx reachable sets

Lemma 8.1 required that the over-approximation sets $\mathcal{R}_t^\epsilon(\{x\})$ be definable for every x and t (see proof). In practice, we need to show that the over-approximation *actually computed by the reachability tool* (which may not be the full ball $\mathcal{R}_t^\epsilon(x)$) is definable. In this section we show that the over-approximations computed by SpaceEx [6] are definable. Given the set $X \subset \mathbb{R}^n$ and finite $\mathcal{V} \subset \mathbb{R}^n$, parameter $\lambda \in [0,1]$ a time step $\delta > 0$, and $(i,j) \in E$, SpaceEx over-approximates $R_{ij}(X)$ by $\mathcal{K}(\mathcal{V}, X) := R_{ij}(TH_\mathcal{V}(X) \cap G_{ij}) \cap Inv(j)$ and $\mathcal{R}_{\lambda\delta}^\epsilon(X)$ by [6]:

$$\begin{aligned} \Omega_\lambda(X,\delta) &= (1-\lambda)X \oplus e^{\delta A}X \\ &\oplus (\lambda E_\Omega^+(X,\delta) \cap (1-\lambda)E_\Omega^-(X,\delta)) \end{aligned} \quad (8)$$

where $TH_\mathcal{V}(X) := \{x \in \mathbb{R}^n \mid \wedge_{\vec{a}\in\mathcal{V}} \vec{a} \cdot x \leq \rho(\vec{a}, X)\}$ is the template hull of X and ρ its support function, $E_\Omega^+ = \boxdot(\Phi_2\boxdot(A^2X)$, $E_\Omega^- = \boxdot(\Phi_2\boxdot(A^2e^{\delta A}X))$, $\oplus$ is the Minkowski sum, $\boxdot S = [-\overline{|x_1|}, \overline{|x_1|}] \times \ldots \times [-\overline{|x_n|}, \overline{|x_n|}]$ is the box hull with $\overline{|x_i|} := \max\{|x_i| \text{ s.t. } x = (x_1, \ldots, x_n) \in S\}$.

Proposition 8.1. *For all definable polytopes $X \subset \mathbb{R}^n$, the sets $\mathcal{K}(\mathcal{V}, X)$ and $\Omega_\lambda(X,\delta)$ is definable are $\mathcal{L}_{\exp}$.*

Proof. Let $S, Y \subset \mathbb{R}^n$ be two definable sets in some o-minimal structure $\mathcal{A}$. Let $\lambda \in \mathbb{R}$ and let A be a real matrix. Then the following sets are also o-minimal: λS, AS, $S \cap Y$, $S \oplus Y$, $S \cap Y$, $TH_\mathcal{V}(S)$ and $\boxdot S$. Now the result follows by noting that $\mathcal{K}(\mathcal{V}, X)$ and $\Omega_\lambda(X,\delta)$ are constructed by composing the above definability-preserving operations. □

9. CONCLUSION

In this paper, we presented the first formalization of a hybrid system model of the human heart and the ICD device and showed that the resulting closed-loop may be formally verified. We showed that the heart model, the ICD measurement process, the modules of common ICD, and the parallel composition of the entire system to be a STORMED hybrid system, which admits finite bisimulation. In the process, we were able to show that approximate reachability yields finite simulation for STORMED systems and that certain composition respect the STORMED property. Finally, we showed that the reach set computed by SpaceEx may be used to build the simulation.

10. REFERENCES

[1] R. Alur, T. A. Henzinger, G. Lafferriere, and G. J. Pappas. Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88(2):971ï£¡–984, 2000.

[2] E. Bartocci, F. Corradini, M. D. Berardini, E. Entcheva, S. Smolka, and R. Grosu. Modeling and simulation of cardiac tissue using hybrid i/o automata. *Theoretical Computer Science*, 410(33):3149 – 3165, 2009.

[3] Boston Scientific Corporation. The Compass - Technical Guide to Boston Scientific Cardiac Rhythm Management Products. *Device Documentation*, 2007.

[4] T. Brihaye and C. Michaux. On the expressiveness and decidability of o-minimal hybrid systems. *Journal of Complexity*, 21(4):447 – 478, 2005.

[5] T. Chen, M. Diciolla, M. Kwiatkowska, and A. Mereacre. Quantitative verification of implantable cardiac pacemakers over hybrid heart models. *Information and Computation*, 236:87 – 101, 2014. Special Issue on Hybrid Systems and Biology.

[6] G. Frehse, C. L. Guernic, A. Donze, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler. Spaceex: Scalable verification of hybrid systems. In *Proceedings of the 23d CAV*, 2011.

[7] M. R. Gold et al. Prospective comparison of discrimination algorithms to prevent inappropriate ICD therapy: Primary results of the Rhythm ID Going Head to Head Trial . *Heart Rhythm*, 9(3):370 – 377, 2012.

[8] R. Hood. The EP Lab. Accessed 10/20/2015.

[9] Z. Jiang, M. Pajic, S. Moarref, R. Alur, and R. Mangharam. Modeling and Verification of a Dual Chamber Implantable Pacemaker. *Tools and Algorithms for the Construction and Analysis of Systems*, 7214:188–203, 2012.

[10] R. Klabunde. *Cardiovascular electrophysiology concepts*. Lippincott-Williams, 2 edition, 2011.

[11] G. Lafferriere, G. J. Pappas, and S. Sastry. O-minimal hybrid systems. *Mathematics of Control, Signals and Systems*, 13(1):1–21, 2000.

[12] D. Mery and N. K. Singh. Pacemaker's Functional Behaviors in Event-B. *Research report, INRIA*, 2009.

[13] A. J. Moss et al. Reduction in inappropriate therapy and mortality through icd programming. *New England Journal of Medicine*, 367(24):2275–2283, 2012.

[14] M. Pajic, Z. Jiang, I. Lee, O. Sokolsky, and R. Mangharam. Safety-critical medical device development using the upp2sf model translation tool. *ACM Trans. Embed. Comput. Syst.*, 13(4s):127:1–127:26, 2014.

[15] P. Prabhakar, V. Vladimerou, M. Viswanathan, and G. E. Dullerud. Verifying tolerant systems using polynomial approximations. In *RTSS*, pages 181–190, 2009.

[16] M. Rosenqvist, T. Beyer, M. Block, K. Dulk, J. Minten, and F. Lindemans. Adverse Events with Transvenous Implantable Cardioverter-Defibrillators: A Prospective Multi-center Study. *Circulation*, 1998.

[17] P. S. Spector. Visible ep. Accessed 10/20/2015.

[18] P. S. Spector, N. Habel, B. E. Sobel, and J. H. Bates. Emergence of complex behavior: An interactive model of cardiac excitation provides a powerful tool for understanding electric propagation. *Circulation: Arrhythmia and Electrophysiology*, 4(4):586–591, 2011.

[19] J. Stinnett-Donnelly et al. Effects of electrode size and spacing on the resolution of intracardiac electrograms. *Coronary Artery Dis.*, 23(2), 2012.

[20] P. Tabuada. *Verification and Control of Hybrid Systems* . Springer, 2008.

[21] K. Ten Tusscher, R. Hren, and A. V. Panfilov. Organization of ventricular fibrillation in the human heart. *Circulation Research*, 100(12):e87–e101, 2007.

[22] L. P. D. van den Dries. *Tame Topology and O-minimal Structures*. Cambridge University Press, 1998.

[23] V. Vladimerou, P. Prabhakar, M. Viswanathan, and G. Dullerud. Stormed hybrid systems. In *Automata, Languages and Programming*. 2008.

APPENDIX

Proof of Lemma 5.3.

Proof. We show the resets are monotonic - the other properties are immediate. The state is $x = (t, L_2, L_1, \kappa, \sigma_2)^T$. The self-transition ACCUMULATE → ACCUMULATE is initiated by VEvent (ventricular peak). At reset time, $0 \leq t \leq DL$, we have that $\phi \cdot (0-t, t^2, t, 1, 0)^T \geq -\phi_1 DL + \phi_4 \overset{Want}{\geq} \zeta$.

The transition ACCUMULATE → FINALIZE, initiated at the end of Duration, saves the value of the variance in σ_2. This reset produces the constraint $\phi_5((L_2 - L_1^2/\kappa)/\kappa) \geq \varepsilon|((L_2 - L_1^2/\kappa)/\kappa)|$. But the quantity in absolute value is itself a variance and so is positive, therefore the constraint is simply $\phi_5 \geq \varepsilon$, compatible with the previous inequality. □

Proof of Lemma 8.1.

Proof. This follows the lines of the elegant proof of [4] as formulated in [20] and generalizes it to set-valued maps. (The fact that using an approximate *Post* operator yields a simulation is a special case of a more general result on transition systems but we prove it here for completeness).

First observe that using approximate reachability on a system $\mathcal{H}$ is tantamount to replacing $\mathcal{H}$ with a system $\mathcal{H}^\varepsilon$ whose flows and reset maps are set-valued ε over-approximations of the flows and resets of $\mathcal{H}$ (but is otherwise unchanged). Therefore define the dynamical system $\mathcal{D}^\varepsilon$ with state space X and whose flow $\Theta : \mathbb{R} \times \mathbb{R}^n \to 2^{\mathbb{R}^n}$ is a set-valued ε over-approximation of θ_ℓ: $\Theta(t;x) = \{y \in \mathbb{R}^n \mid ||y - \theta(t;x)||^2 \leq \epsilon^2\}$. Let $\mathcal{P} := X/\sim$ be the partition induced by $\sim$. It follows from the definability of θ and $||\cdot||^2$ that Θ is definable. Given $P \in \mathcal{P}$, let $Z(P) = \Theta^{-1}(P) := \{(x,t) \mid \Theta(x,t) \cap P \neq \emptyset\}$. Then $Z(P)$ is definable because P and Θ are definable. Let $Z_x(P) = \{t \mid (x,t) \in Z(P)\} \subset \mathbb{R}$ be the *fiber* of Z over x. The number of connected components of $Z_x(P)$ equals the number of times that $\Theta(x,t)$ intersects P. Now it follows from [20] Thm.7.11 that there exists a uniform upper bound on the number of connected components of $Z_x(P)$, independent of x. Let that bound be V_P. Thus $\Theta(x,t)$ visits P at the most V_P times, regardless of x. Since there is a finite number of blocks $P \in \mathcal{P}$, then $\Theta(x,t)$ visits any block P a maximum of $V := \max_P(V_P)$ times.

Thus we can associate to each $x \in X$ a finite number of finite strings $q(x) = (\ell_1, \ell_2, \dots, \ell_{i-1}, \widehat{\ell_i}, \ell_{i+1}, \dots, \ell_s)$, where $\ell_i, \widehat{\ell_i} \in \mathcal{P}$. Each $q(x)$ gives the sequence of blocks that $\Theta(x,t)$ visits (with repetition), and in which $\widehat{\ell_i}$ is the block containing x. There may be more than one such string because the set $\Theta(x,t)$ might intersect more than one block of $\mathcal{P}$ at a time. The length of $q(x)$ is thus uniformly upper-bounded by $V \cdot |\mathcal{P}|$, so there's a finite number of different strings $q(x)$. Let $\mathcal{Q}(x)$ be the set of such strings associated to x, and let $\mathcal{Q} = \cup_x \mathcal{Q}(x)$. Then $\mathcal{Q}$ is the state space of the finite transition system $K = (\mathcal{Q}, \{*\}, \to, \mathcal{Q}_0)$ whose transition relation is

- $\ell_1 \dots \widehat{\ell_i} \dots \ell_s \xrightarrow{*} \ell_1 \dots \widehat{\ell_{i+1}} \dots \ell_s$
- $\ell_1 \dots \ell_{s-1} \widehat{\ell_s} \xrightarrow{*} \ell_1 \dots \ell_{s-1} \widehat{\ell_s}$

It is clear that K is non-deterministic and simulates $\mathcal{D}$ but is not a bisimulation because of the over-approximation produced by Θ. □