EPiC Series in Computing

Volume 43, 2017, Pages 9–17

ARCH16. 3rd International Workshop on Applied Verification for Continuous and Hybrid Systems

Hybrid Automata Model of the Heart for Formal Verification of Pacemakers (Benchmark Proposal)

Sidharta Andalam[1], Avinash Malik[1], Partha S Roop[1], and Mark Trew[2]

[1] Department of Electrical and Computer Engineering, University of Auckland, New Zealand
{sid.andalam, p.roop, avinash.malik}@auckland.ac.nz
[2] Auckland Bioengineering Institute, University of Auckland, New Zealand
m.trew@auckland.ac.nz

Abstract

A cardiac model of networked Hybrid Automatas (HAs) cells or nodes is potentially very useful for industry validation of pacemaker algorithms. Such a model replicates the electrical conduction system of the heart and the interaction with a pacemaker. The benchmark is a network of more than 100 HAs. It is based on a published model[1]. It exhibits several key phenomena that are typical for hybrid systems and reachability analysis.

Category: academic **Difficulty:** high[2]

1 Context and Origins

Artificial cardiac pacemakers are embedded devices that stimulate the heart with electrical impulses to maintain or restore a normal rhythm in people with a slow or irregular heart rate. These devices continuously monitor a human heart and must operate in a fail-safe manner all the time. However, in 1990-2000, close to 200,000 pacemakers were recalled due to software related failures [2]. As the complexity of the pacemakers increase, there is a need for the development of better processes for validation of such medical devices.

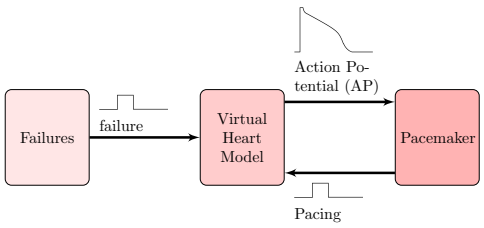
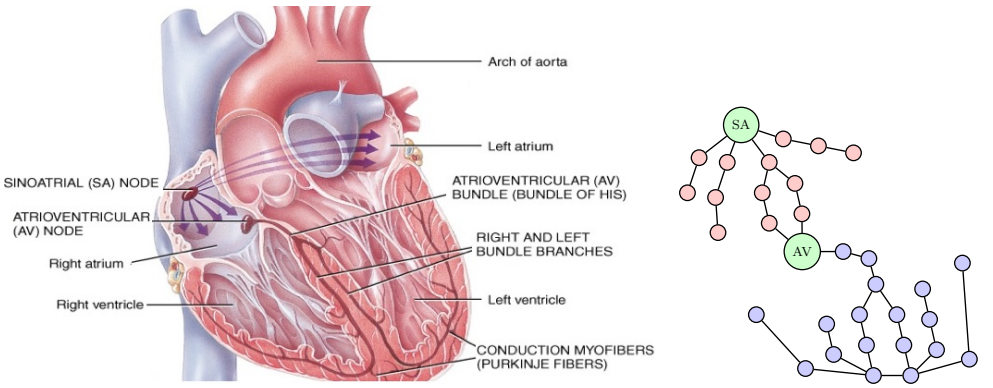


Figure 1: Overview of the closed-loop system to verify

[1] Authors express their gratitude to the research group of Prof. Marta Kwiatkowska for sharing their Simulink® heart model reported in [3], which was foundational in developing the benchmark

[2] Indicate as appropriate: category (academic, industrial), difficulty (low, medium, high, challenge)

In this paper, we develop a case study for validating pacemakers. Figure 1 presents the overview of the approach. The virtual heart model captures the electrical conduction system of a heart. It is the job of the pacemaker to continuously monitor the heart and pace it when required. We can also dynamically configure the heart to exhibit some failure conditions which the pacemaker needs to overcome to maintain consistent heart rate.



(a) Diagram of the heart. Reproduced from [1]

(b) An abstracted model of the heart

Figure 2: Electrical conduction systems of the heart

2 Background

Using Figure 2, we explain the electrical conduction system of the heart which is responsible for controlling the timing of the heartbeats. During each beat, (see Figure 2(a)) electrical signals travel through the network of conducting cells to contract and relax the heart. The source of the signal is the Sinoatrial (SA) node, which is the natural pacemaker located in the right atrium. The electrical signal propagates through the right and left atria, contracting the muscles and moving the blood into the ventricles. To ensure both ventricles are filled, the Atrioventicular (AV) node introduces critical delay in the conduction system. Finally, the signal travels through both ventricles. This contracts the muscles and pumps the blood out of the heart.

The human heart has over two trillion cells. For analytical purposes, an abstract model based on Timed Automata (TA) consisting of a network of 33 nodes (or cells) has used for testing off-the-shelf pacemakers [6]. A more refined approach that models the continuous voltage using Hybrid Input Output Automata (HIOA) is presented in [3]. In both cases, the abstraction from two trillion cell to 33 nodes is not discussed in the literature. The abstracted model consisting of nodes and paths is presented in Figure 2(b). In the next section, using Hybrid Input Output Automata (HIOA) [3], we describe the cell's electrical behaviour.

3 Modelling the cell behaviour

An electrical signal driving heart contraction is generated by the transfer of ions across the cells membrane. This change is described as the Action Potential (AP) [3] (see Figure 3(b)). It can

be described in four phases : (0) Resting Period (RP), (1) Stimulated (ST), (2) Upstroke (UP) and (3) Effective Refractory Period (ERP). More details are available in [3].

A cell is connected to a neighbouring cell using a *path* which delays the voltage signal propagation between cells. For each cell, the four phases of the action potential are mapped to four locations ($q_0 - q_3$) of the HIOA, see Figure 3(a). The variable v is the voltage, i_{st} is the stimulus current, C_1 to C_5 are constants and V_R, V_T and V_O are the threshold voltages depicted in Figure 3(b). The symbol θ captures how early a cell is re-excited before it is completely rested, this affects the morphology of the action potential in location q_3 which is dictated by the function $f(\theta) = C_3 \times v \times (1 + 13 \times \theta^{1/6})$, as described in [3]. Finally, for this benchmark we simplify the influence of neighbouring cells voltage to an input gv. It is defined as $gv = \sum_{i=1}^{N} v_n \times A - v \times B$, which captures the difference in neighbouring (v_n) and the voltage, v, of the current cell. Here, A and B are constant parameters that capture the attenuation of the voltage signal.

4 Modelling in SpaceEx

SpaceEx is a verification tool for hybrid systems [4]. An overview of the benchmark is presented earlier in Figure 1. A top-level implementation of the benchmark in SpaceEx is presented in Figure 4. In this section, we first linearise the model such that it is accepted by SpaceEx. Then, we present the SpaceEx models of the cell, the heart, the pacemaker and the induced failures. We discuss some of the limitations of the tool in effectively describing the models.

4.1 Linearisation

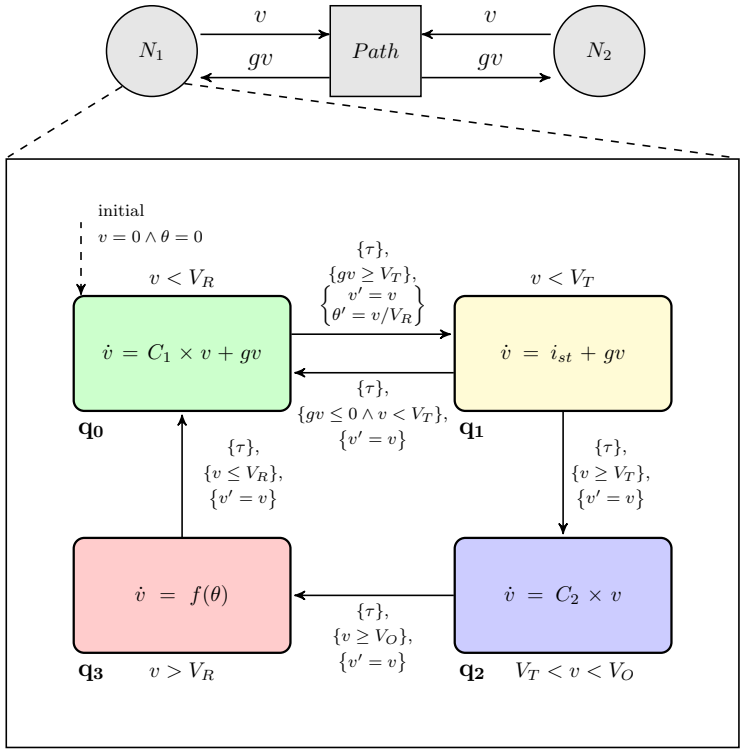
SpaceEx restricts the flow constraints on a continuous variable to the form : $\frac{d}{dt}x = Ax + Bu + b_0$, where x is a continuous variable, u is a non-deterministic inputs and A, B and b_0 are constants. Further, the assignments are restricted to the forms $x := Ax + Bu + b_0$. To satisfy these constrains, for our benchmark, we approximate the function $f(\theta, v) = C_3 \times v \times (1 + 13 \times \theta^{1/6})$ to $f(\theta) = C_4 + C_5 \times \theta$ using curve fitting. This approximation affects the morphology of the cell's action potential, see Figure 3(b). The impact of this approximation on the behaviour of the heart is not studied in this paper.

4.2 Cell model

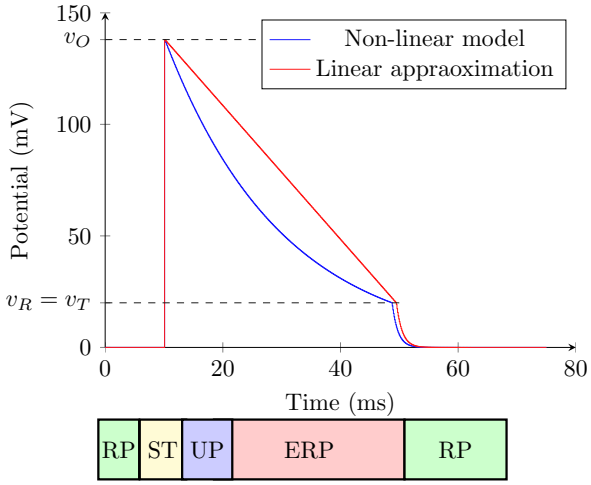
For the HIOA model of the cell described in Figure 3(a), the model in SpaceEx is presented in Figure 5(a). To reduce the non-determinism, the implementation in SpaceEx has more constraints. For example, in location q_0 of Figure 3(a), the invariant ($v < V_R$) and the guard ($gv \geq V_T$) are independent and both can be enabled leading to non-determinism. This model is accepted by SpaceEx. However, to reduce non-determinism and improve scalability (and reflect the real behaviour of the cell), we add further constraints as seen in location q_0 of Figure 5(a). The results of the reachability analysis on the output voltage of the cell is presented in Figure 5(b). The morphology of the curve resembles the action potential in Figure 3(b).

4.3 Path model

Figure 2(b) presents the network of nodes and paths. Each path captures the prorogation delay of the continuous signal between two nodes. In [3], the path is not described as HA but, is captured using Simulink's Transport Delay module which is a FIFO buffer. The size of the



(a) HA model of cell's Action Potential (AP). For the non-linear model the function $f(\theta, v) = C_3 \times v \times (1 + 13 \times \theta^{1/6})$. For the linear model the function $f(\theta) = C_4 + C_5 \times \theta$



(b) Morphology of Action Potential (AP)

Figure 3: Action potential of a cell

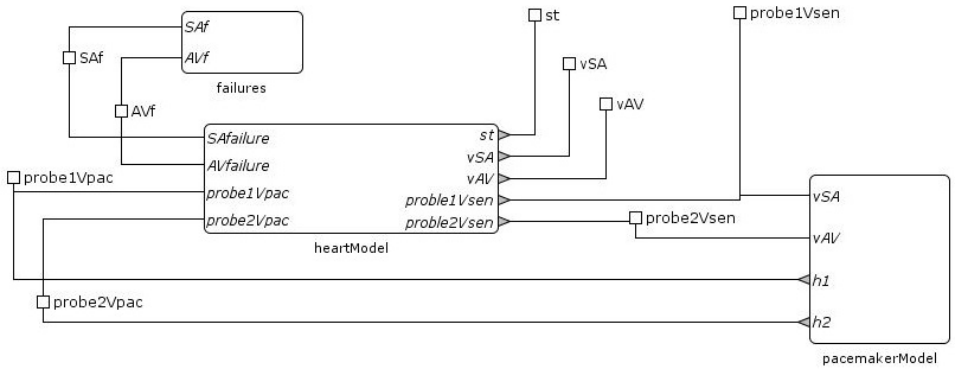


Figure 4: Top-level system implementation in SpaceEx

buffer along wiht the simulation step-size dictates the propagation delay. However, this is it more challenging to model this in SpaceEx. For this benchmark, the path model is presented in Figure 6. It delays the input signal by one simulation cycle/run. Having multiple instances of these in series can allow us to capture the propagation delay between nodes. However, this will significantly increase the number of automata and affects the scalability of the application. Thus, for this benchmark we simplified all paths to a fixed delay and modelled with a single HA.

4.4 Heart model

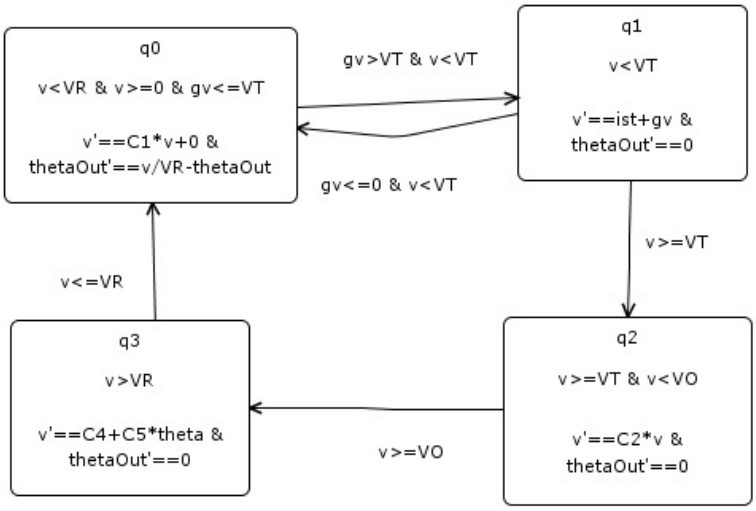
Given the network of nodes in Figure 2(b), Figure 7 presents the SpaceEx model. It captures every node and path separately and maintains traceability. Further, a natural pacemaker to the SA node is added to allow the heart to function without the help from pacemaker. This natural pacemaker can be deactivated by switch *sw1*, if the the input signal *SAfailure* is active (triggered by the component *failure*). Also, two probes (near SA and AV nodes) are introduced to provide interface with the pacemaker

4.5 Pacemaker model

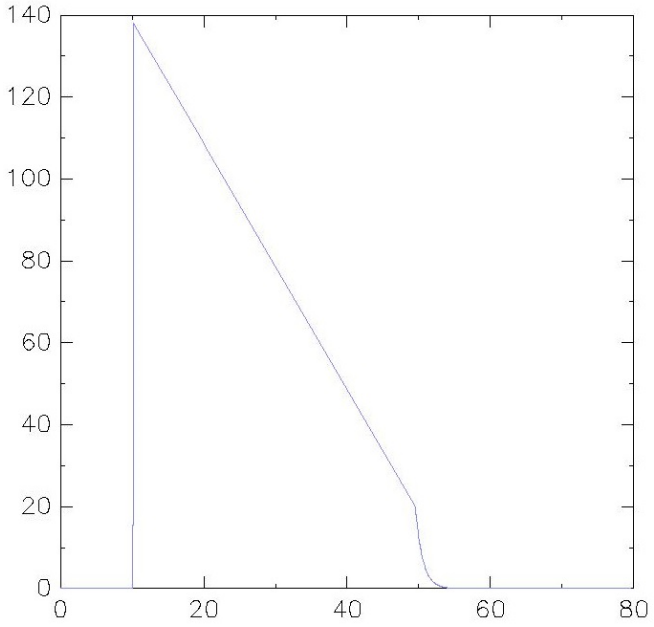
The purpose of the pacemaker is to treat any abnormal heart rhythms. For example, to speed up a slow heart. Some possible scenarios that lead to the abnormal behaviour and the required action from pacemaker are presented in the Table 1. The first scenario, when the natural pacemaker of the heart stops working, the pacemaker detects it by simply observing the voltage on the probe (*probe1Vsen*) and activating the heart (*probe1Vpac*) when required. The behaviour is captured using the hybrid automaton in Figure 8. Here, input *vSA* (voltage after cell SA) and output h (pulse from the pacemaker) are mapped to *probe1Vsen* and *probe1Vpac*, respectively. Similarly, the second scenario, for AV node is implemented. More expressive scenarios such as detecting Endless Loop Tachycardia can be added to the pacemaker model. Some of these complex scenarios are presented in [5].

4.6 Verification results from SpaceEx

Due to scalability issues, we were only successful in completing reachability analysis for the voltage of a singe cell. This result is captured in Figure 5(b). On a Windows PC with Intel i7



(a) cell model



(b) Morphology of AP (reachability of voltage v)

Figure 5: Modelling the cell in SpaceEx

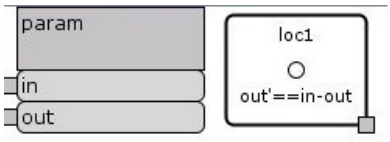


Figure 6: Modelling the path in SpaceEx

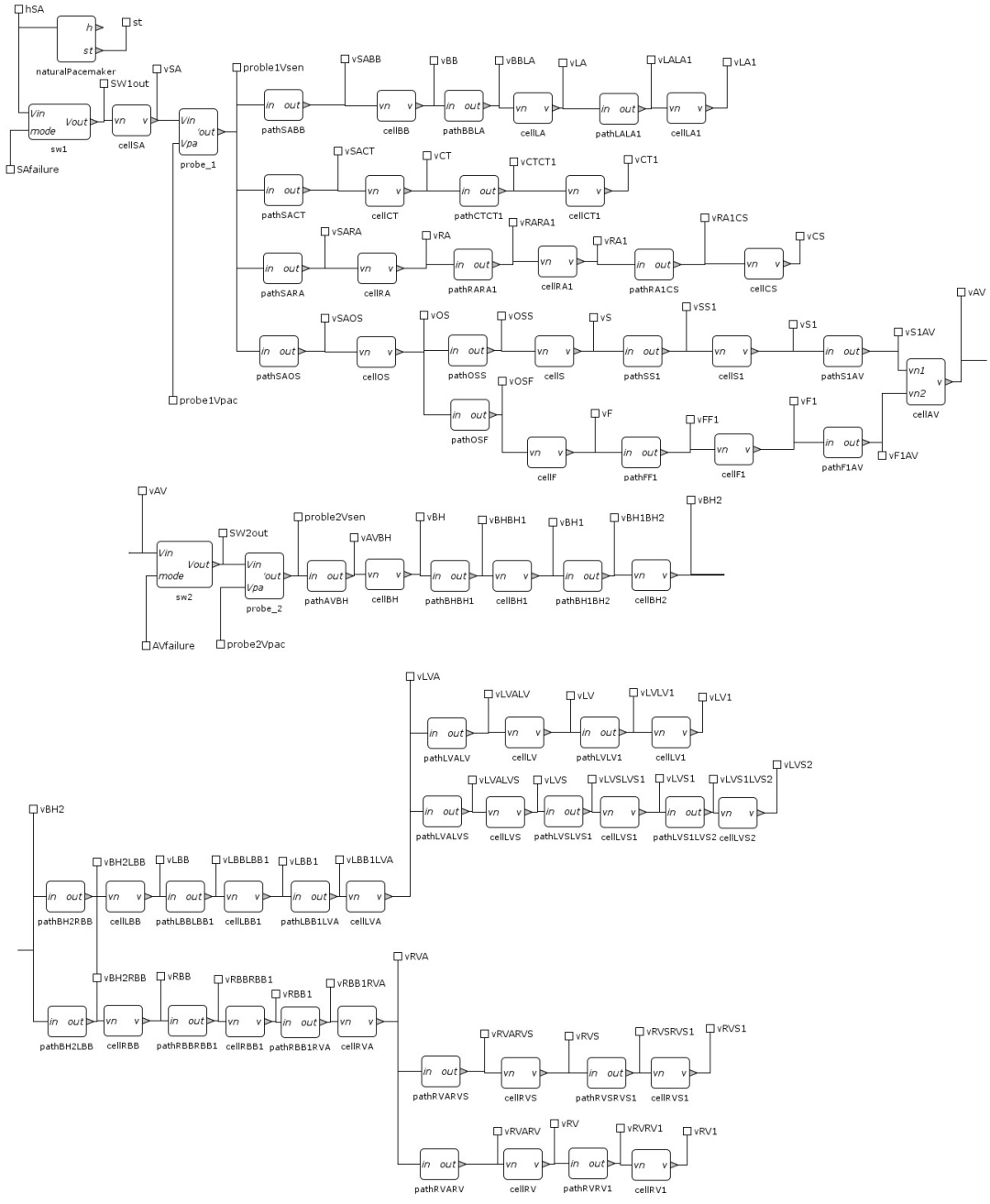


Figure 7: Modelling the heart with 33 nodes and the connecting paths from Figure 2(b)

Heart problem	Pacemaker fault detection	Pacemaker action
Natural pacemaker stopped working	Voltage from probe *probe1Vsen* is less than the *SAthreshold* for a period longer than *SAinterval_1*	Stimulate the heart by activating probe *probe1Vpac* for a period of *SAinterval_2*
AV node does not conduct	Voltage from probe *probe2Vsen* is less than the *AVthreshold* for a period longer than *AVinterval_1*	Stimulate the heart by activating probe *probe2Vpac* for a period of *AVinterval_2*

Table 1: Pacemaker properties

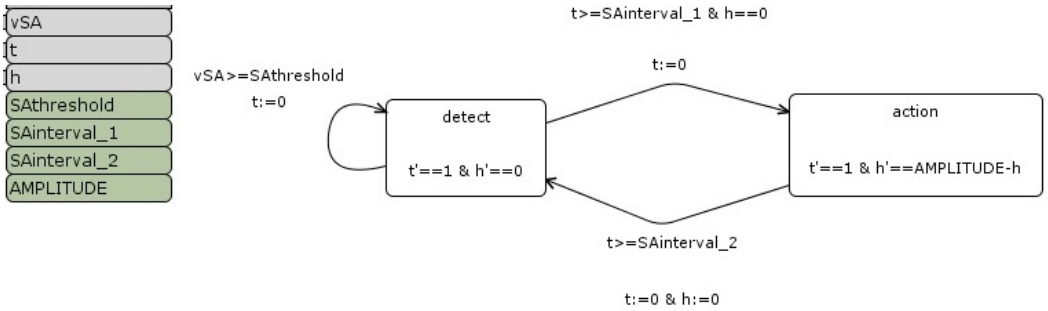


Figure 8: Fault detection and the action taken by the pacemaker

and 16 GB memory, the tool ran out of memory in 3 minutes while verifying the entire heart. Some other properties, that would help validate the pacemaker are as presented in Table 2. Variables t1 and t2 measure the duration between two consecutive activations of SA and AV nodes, respectively.

Heart behaviour	Forbidden states in SpaceEx
Always the heart is in the working range i.e., the duration between any two consecutive beats is within the accepted range	$t1 \leq MIN\_DURATION$ & $t1 \geq MAX\_DURATION$ & $t2 \leq MIN\_DURATION$ & $t2 \geq MAX\_DURATION$

Table 2: Verification properties

More expressive scenarios such as detecting Endless Loop Tachycardia can be added to the heart and the pacemaker models. Some of these complex scenarios are presented in [5]. This is part of our future work for improving this benchmark.

5 Conclusions and recommendations

Modelling and verification of biological systems poses a challenging problem for formal verification. In this benchmark, we present a case study for validating a cardiac pacemaker. The benchmark consists of a virtual heart in closed-loop with a pacemaker. The model consists of more than 100 HAs, although we were not successful at describing the path delay which simply delays the analogue voltage signal. We hope this benchmark is useful for verification tool developers for validating the scalability of their tool and adding new features.

References

[1] THE CONDUCTION SYSTEM. http://monashparamedicnurse.weebly.com/w1-cardiac-anatomy–physiology-review.html. last accessed - 27.01.2016.

[2] H. Alemzadeh, R. K. Iyer, Z. Kalbarczyk, and J. Raman. Analysis of safety-critical computer failures in medical devices. *Security & Privacy, IEEE*, 11(4):14–26, 2013.

[3] 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.

[4] G. Frehse, C. L. Guernic, R. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, and T. Dang. SpaceEx: Scalable verification of hybrid systems. In *In Proceedings of the International Conference on Computer Aided Verification*, 2011.

[5] Z. Jiang, M. Pajic, S. Moarref, R. Alur, and R. Mangharam. Closed-loop verification of medical devices with model abstraction and refinement (submitted). *International Journal on Software Tools for Technology Transfer*, 2013.

[6] M. Zhihao J, Pajic and R. Mangharam. Cyber Physical Modeling of Implantable Cardiac Medical Devices. *Proceedings of the IEEE*, 100(1):122–137, 2012.