Reviews

Dear Houssam,

Thank you for your submission to HSCC 2016. The HSCC 2016 review response period will be between today and December 5 (AOE: Anywhere On Earth). This email concerns the paper titled:

\*Model checking Implantable Cardioverter Defibrillators\*

\* The response must focus on any factual errors in the reviews and any questions posed by the reviewers. It must not provide new research results or reformulate the presentation. Try to be as concise and to the point as possible.

\* The response should not exceed 750 words.

----------------------- REVIEW 1 ---------------------

PAPER: 63

TITLE: Model checking Implantable Cardioverter Defibrillators

AUTHORS: Houssam Abbas, Kuk Jin Jang, Zhihao Jiang and Rahul Mangharam

----------- REVIEW -----------

The paper presents theoretical results on the verification of implantable defibrillators (ICD) using a model-based approach. The authors define detailed hybrid automata models that describe the key components of the system: a cellular automata-based model of the electrical conduction system (formalised from existing work), together with sensing and arrhythmia detection components. This work focuses on STORMED hybrid systems, an expressive class of hybrid systems defined over o-minimal structures and with additional restrictions that ensure "well-behaved" paths. This entails the existence of finite bisimulations, thus enabling model checking. For each introduced model, the authors systematically prove compliance to the STORMED class. However this is not enough to ensure that their composition is STORMED, so an additional condition on the overall system is formulated and further demonstrated to guarantee the STORMED proprieties. To deal with the difficulty of computing exact r!

each sets, the authors examine approximate reachability methods/tools (based on SpaceEx), showing that they can be used to build a simulation/abstraction of the system.

With the definition of the first formal model for ICDs and the demonstration that this can be formally verified, opening for development of model checking tools, the paper makes a relevant contribution to the rigorous design of medical devices. Therefore, I recommend acceptance.

In revising the manuscript, I suggest taking into account the following comments.

General comments (mainly about the heart model)

- Due to the nature of the work, models are just defined and not evaluated/simulated, so it's not possible to understand if the proposed heart model is suitable enough to ICD verification. The authors should better motivate this choice, especially discussing if this model has been already used in past work to reproduce fibrillation. If not, how/for which parameters can it be reproduced? Moreover, how do you compare this model with the more established ones based on ion currents?

- What is the number of cells considered in the original CA model? It seems to me that this could represent a limitation to practical model checking due to the high number of components (cells) that could be required for accurate modelling of the conduction system. I recommend discussing this aspect.

- Given the "abstract" presentation of the model, I believe the heart model can be improved (without compromising STORMED properties) in order to consider more general cell topologies. I would discuss this if authors think is relevant.

- How the ICD automata relate to the original Boston Scientific specification? Do they need validation from domain experts?

- The model checking tools you aim to develop in future will be tailored for ICDs or could support more general STORMED systems?

Detailed comments

- Figures 1 and 2 appear much earlier the point they are referred to. Consider postponing.

Abstract:

- "Model-based verification can play a crucial role in ICD development." this is clearly the case but should be motivated with a short sentence after/before in the text.

- "show that it admits a finite bisimulation by showing it to be a STORMED hybrid system". explain briefly what STORMED systems are, and why you consider them.

- "The results of this paper are theoretical...". Not just, you define also new models.

- "In future work we will implement a procedure for model checking the heart+ICD loop." I personally don't like future intentions in the abstract. This should go in a conclusion/future work section. I suggest to rephrase, writing e.g. "the theoretical results open for the implementation of concrete model checking procedures..."

Introduction:

- Related work seems a bit partial. I also suggest discussing literature in the verification of similar kinds of hybrid systems. Especially since you tell that abstractions will be probably unavoidable, you could select a number of approximate methods for the verification of related systems.

- "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." a bit too loose connection. Motivate more why spaceex, e.g. because you plan to use it in the model checking tool? as an example, to show that the theoretical framework accommodates state-of-the-art techniques for approximate reachability?

- "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." same comment as in the abstract

- "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." and of course, don't forget to remove this paragraph

Section 2:

- Definition 2.6 is a bit imprecise. I know it is taken from the original paper, but there, monotonicity precedes the definition, so that worked. I mean that you should tell before the (S) condition that $\epsilon$ and $\zeta$ are positive reals.

Section 3:

- "i) the ICD will always reach a decision of VT or SVT in finite time" It doesn't seem you have introduced before the acronyms "VT" and "SVT".

- "at which point it flushes its variables so new values are ..." this sentence is not clear to me. Consider rephrasing.

- "inn Fig. 3, $V(i,j,t) \in \mathbb{R}$ denotes the voltage in cell $(i,j)$ of the grid at time $t$, and vector $V = (V(1,1),...,V (N^2,N^2))^T$"...shouldn't the vector be denoted as "$V = (V(1,1,t),...,V (N^2,N^2,t))$"?

- "The APD restitution mechanism of heart cells,..." is the APD acronym introduced earlier?

- Proof of theorem 3.1: "(ED) holds by Lemma 2.1", you mean proposition 2.1, or you want to change prop. 2.1 to a lemma

Section 4

- "$\overset{Want}{\geq}$" Can you explain this notation?

Section 5

- Proof of lemma 5.2: "Separability obtains by observing" is obtained by observing?

----------------------- REVIEW 2 ---------------------

PAPER: 63

TITLE: Model checking Implantable Cardioverter Defibrillators

AUTHORS: Houssam Abbas, Kuk Jin Jang, Zhihao Jiang and Rahul Mangharam

----------- REVIEW -----------

SUMMARY

The paper focuses on the model checking of a cardiovascular medical device (ICD). It proposes the first hybrid automata modeling of the closed-loop system (heart + sensing device + ICD), and it proves that the model belongs to the class of Stormed Hybrid Systems (SHS).

The result is interesting because it proves that the transition system associated to such formalism admits a "finite bisimulation". An SHS admits a finite bisimulation in the sense that a (possibly terminating) algorithm exists to compute it. Despite the finiteness of such procedure, in general, it is not always possible to compute a finite bisimulation due to the undecidability of the underlying theory.

The paper introduces the problem and the necessary background; it defines the SHS's associated to the components of the system and proves that they are STORMED; then, it provides the result that SHS are closed under parallel composition; finally, it shows that for SHA a finite simulation is computable if an over-approximated Post operator is definable.

Since the paper employs an undecidable o-minimal structure (R,<,+,-,dot,exp)

(the theory), only a "finite simulation" might be computed.

CONTRIBUTION

The paper presents a purely theoretical contribution; it does not

provide any experimental result or implementation.

Three contributions are claimed by the authors.

. the paper presents the first hybrid model of the heart + sensing + ICD loop adopted by major ICD manufacturers. This is proved to be a STORMED system.

. a general result about the parallel composition of deterministic SHS, namely, that under the "Collection Separability" condition the SHS are closed under parallel composition.

. a theorem stating that SHS admits a finite simulation if a definable over-approximated Post-operator replaces the exact one.

RELEVANCE

The work is clearly relevant for HSCC, since it focuses on the modeling of an important practical hybrid system, and builds to achieve its future verification.

NOVELTY

The work appears to be novel. The paper reuses existing results on SHS, although the Separability Condition of the original work [23] is relaxed. It is not clear how such modification impacts the SHS properties. It is not clear what is the novelty of th.8.1 w.r.t. state-of-the-art. The related works presented in the paper focuses on pacemakers.

SIGNIFICANCE

The contributions of the paper are clearly stated. However, the significance is hard to evaluate. The paper starts as a kind of case study on ICD devices, and shows how the model falls within an interesting class. Then it proves some properties of SHS. However, the case study is not completely worked out, since no model checkers exist for the SHS class. Neither implementation nor experimental evaluation are given. One could see this as a first important step, or as a submission in a preliminary state.

Except for the general contribution on SHS composition, the work provides models for a specific problem in the cardiovascular domain and just provides the preliminary conditions to model check ICD medical devices.

TECHNICAL ACCURACY

The notation is not uniform and coherent throughout the sections. Some assumptions about the discrete transition semantics seem implicitly used. Some definitions are not accurate. It is not clear if the contribution about the existence of a finite simulation for SHS is valid despite the STORMED property. See Additional comments.

QUALITY OF PRESENTATION

The paper is well organized. The readability of the paper should be improved - currently it suffers from a low technical accuracy. It is difficult to check the coherence between graphical representation of SHS and the corresponding textual descriptions.

ADDITIONAL COMMENTS

1) Section 2 provides the necessary background. In particular, subsection 2.2

defines SHS. The Separability Condition is relaxed (S) w.r.t. the

original definition in [23]. Are the results stated in [23] still valid?

For instance, the new condition allows two Guard Sets to overlap in the

same discrete location whereas the original condition did not.

2) In the formula (3) about s(t):

- the norm function ||.|| , not defined previously, seems applied to a

difference between two pairs (i,j) of integer indexes. What is the

intended semantics?

- About the norm function, in general it might be equal to zero.

This would cause a coefficient equal to infinite. How is this case

handled?

- In the textual description of the signal s(t) it should be the

difference between the electrode potentials, namely V(i,j,t).

Instead, the formula (3) contains the first derivative \dot(V)

of the potentials functions.

3) In section 4, the absolute value |.| is used to define y(t)=|s(t)|.

The first and second derivatives of y are used to detect peaks, but

y(t) is non-differentiable at s(t)=0.

4) Reset Monotonicity and state space boundedness

In section 3, it is stated that the state space is intuitively

bounded because both the electrical potential V and the time horizon t

are bounded.

In figure 3, the time variable t seems monotonic and never reset.

Is the state space X of the shown automaton really bounded?

I would expect some kind of reset t<-0 on the edge phase3RRP -> phase4,

but probably such reset would brake the Reset Monotonicity property.

MINOR POINTS

- the graphical representations of HAs do not show invariants.

- probably the discrete transitions are implicitly supposed to be URGENT.

The semantics of the guards should be better defined to respect the

textual description.

- the graphical representation is not detailed, so it is difficult to

check the coherency of the proofs about STORMEDness.

- some formula is not understandable (e.g. s(t) formula 3 on page 4).

- the notation is confused especially in section 5.2 and 7.

- section 6 tries to exemplify some properties of interest. Even if the

general idea might be deducible, some improvement is needed.

- the definition 2.3 of HA does not define Guards and Reset Functions.

- the distance and norm function are not defined w.r.t. the vector space.

- some reference is missed (e.g. page 5, th3.1, formula (4) )

- Lemma 5.2, condition R1. the last term 1-w is missed in the first vector.

- Lemma 5.2, condition R2. a dot product is used in place of the multiplication (s s\_m)

- Section 5.3. The variance formula is different from the formula shown

in the figure 10, DurationEnds edge. Probably the latter is the correct one.

- th. 7.1 is not clear. Who is x\_j in d(x\_j,...)? does e' belong to E\_i?

- th. 7.1 refers to "deterministic SHS" but it has not been introduced previously.

- Definition 2.3. The transition system associated to a HA does not

constraint the discrete transitions to respect the invariants.

----------------------- REVIEW 3 ---------------------

PAPER: 63

TITLE: Model checking Implantable Cardioverter Defibrillators

AUTHORS: Houssam Abbas, Kuk Jin Jang, Zhihao Jiang and Rahul Mangharam

----------- REVIEW -----------

The paper presents an interesting case study (an implantable cardioverter defibrillator) and some

interesting theoretical developments on STORMED hybrid systems. However, as noted by the authors

themselves, the latter cannot be applied to the former as no tools actually support model checking

STORMED systems. As much as I appreciate the merit of making such confession upfront in the

abstract, the rest of the paper still reads as if the problem of formally verifying this important

health critical system was solved or on the verge of being solved, which I am quite skeptical

about. Even assuming a model-checker for STORMED systems existed or could be easily implemented, I

doubt it would work well on the system described, which looks quite complex and high dimensional to

me. My concern is that finite abstraction is often not enough to guarantee scalability, as experienced by the

similar approaches around approximate bisimulations (btw, some references are missing, e.g., what about

"Compositionality Results For Cardiac Cells Dynamics" by Islam et al, CMSB 2013 ?).

As a consequence, it is difficult to decide what to take away from this paper as to me it

feels like a work-in-progress investigation: the authors attacked the problem in the STORMED

angle, which is maybe a reasonable thing to do, but this has not yet produced concrete results, not

even reasonably promising indications that there will be eventually. There are some interesting

ideas, such as leveraging a scalable reachability analysis tool (Spaceex) but the description of

this seems also quite preliminary. Also, why not applying directly (or more directly) such a tool to

the problem without trying to prove o-minimality and bi-simulation results? All in all, I think with

the current status of the work, the paper would be better suited as a case study paper, focusing

more on the description of the problem, which is certainly of interest for the community, but

leaving aside the theoretical developments until some more concrete results are obtained.

Review 4

------------

The paper aims to develop an approach for formal verification of Implantable Cardioverter Defibrillator (ICD) devices by creating a simulation of the device (and an appropriate model of the heart) with a STORMED hybrid system. To this end, the authors show that the chosen model is a STORMED system and more generally that STOREMED systems are closed under composition under an assumption about pair-wise separation of guards. It does not quite go all the way to perform verification of the target system citing that there are no practical verifiers available for STORMED models.  
  
The theoretical contribution of the paper is in Theorem 7.1 which shows that STORMED automata are closed under composition under an assumption called collection separability. This restriction as is it is stated did not make sense to me. What is the relationship between the state components x\_i and x\_j? If they are independent (as is usual in product constructions) then how does x\_i \in G\_e^i give information about x\_j ? If they are not independent, say, components of reachable states of the composition then Theorem 7.1 has to be changed appropriately. Also, the index variable k is left free in the statement of the theorem. It is also not clear, why the authors have chosen to define a general m-ary composition operator instead of the usual binary composition, which can then be applied inductively.  
  
The interesting point in the case study is that the behavior of the voltage of an individual cardiac cell is not monotonic (voltage goes up and down with the action potential), yet, the authors show that by looking at the overall state of the model that includes a couple of timers, it is possible to show that the flows and resets are monotonic with respect to a fixed direction. This construction is inside the proof of Theorem 3.1, and it would be useful to elaborate and discuss possible generalizations.  
  
Although the ICD reaches a decision VT or SVT within a finite time window, why is it reasonable to assume that the variables are all reset after that window? The cell membrane has hysteresis (memory) from the last potentiation. In fact, Grosu et al. [HSCC 2007] and other papers took great pains to model this behavior with what they called Cycle-Linear Hybrid Automata. Some further discussion about this is needed.  
  
The discussion of work related to STORMED automata is adequate. As for the main application area of cardiac device verification, comparison of the results in the relevant papers by Huang et al. (e.g., from CAV 2014) and Grosu et al. that work with similar 2D hear models should be included. Citation [1] has typos. [17] is incomplete.