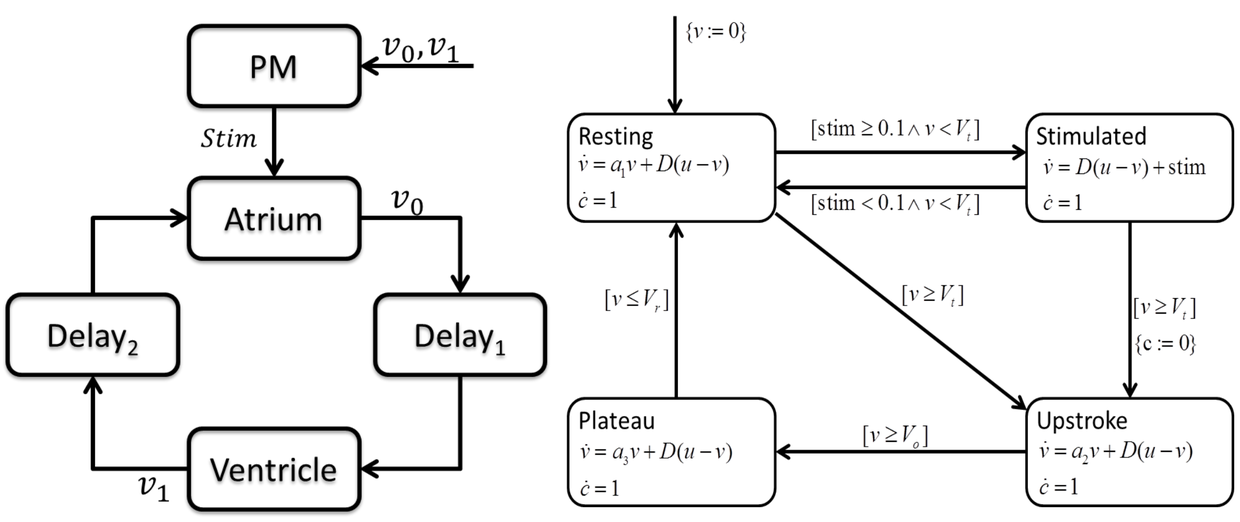
Automatic Safety Verification of Implantable Medical Devices

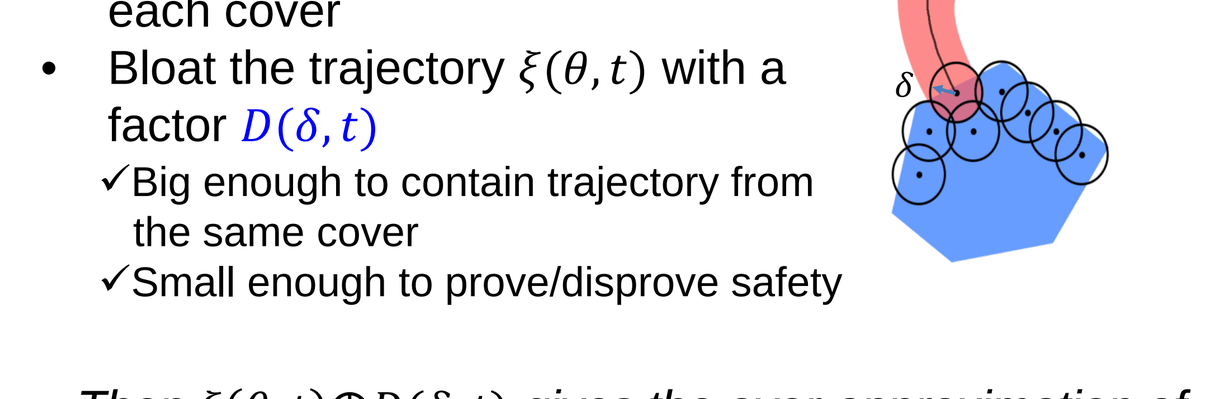
Zhenqi Huang, Chuchu Fan, Alexandru Mereacre,
Sayan Mitra and Marta Kwiatkoska

The testing and verification of medical devices pose numerous challenges due to continuous interactions between the physical processes and software, delays, and uncertainty. This research describes a framework based on simulation and compositional analysis for investigating and validating safety of implanted pacemakers.

Model of the pacemaker-heart interface



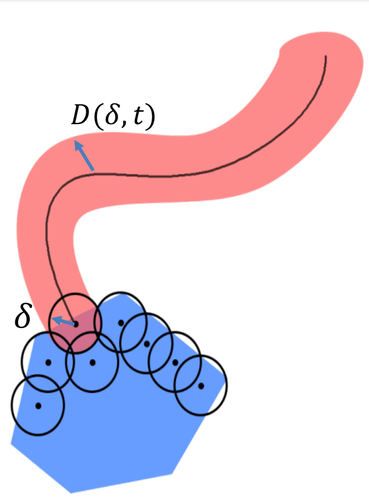
Heart-pacemaker interface: Atrium and Ventricle are oscillators with 4 phases each. v_0, v_1 capture the voltages of atrium and ventricle. They send pulses to each other with **nondeterministic delays**. The pacemaker (PM) senses these pulses, and sends a stimulus if the interval between two pulses is lower than a design parameter LRI



Goal: choose LRI such that heart rate is always in acceptable range, despite nondeterministic delay & initial state.

Simulation-based compositional verification

- Create a finite cover of the parameter/initial space
- Simulate a trajectory $\xi(\theta, t)$ from each cover
- Bloat the trajectory $\xi(\theta, t)$ with a factor $D(\delta, t)$
  - ✓Big enough to contain trajectory from the same cover
  - ✓Small enough to prove/disprove safety



Then $\xi(\theta, t) \oplus D(\delta, t)$ gives the over-approximation of reachable set from the cover.

Compositional discrepancy computation

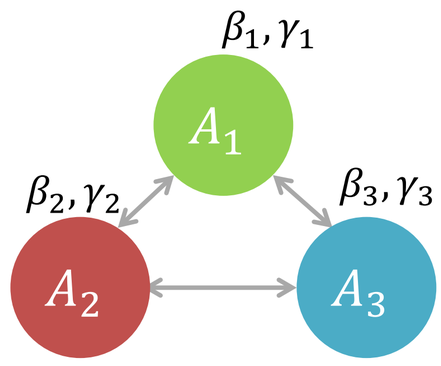
Using component-level property IS-discrepancy to compute the function $D(\delta, t)$

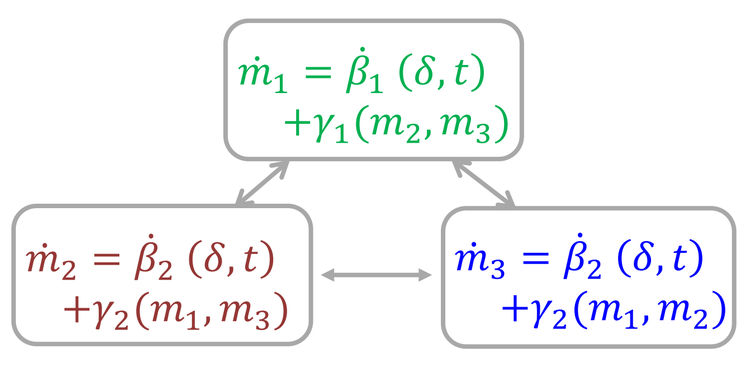
Definition. **IS-discrepancy** of a component is defined by two functions β and γ such that for any initial states θ, θ' and any inputs u, u',

$$|\xi(t) - \xi'(t)| \leq \beta(|\theta - \theta'|, t) + \int_0^t \gamma(|u(s) - u'(s)|) ds$$

ξ, ξ' are the trajectories corresponding to (θ, u) and (θ', u')

- We provide on-the-fly method to compute IS-discrepancies
- Using the IS-discrepancies of the components, construct a **small model approximant**
- The trajectory of the small model gives $D(\delta, t)$
- The model can be constructed dynamically with different connection topologies and delays





Experimental results

LRI	Delay1	Delay2	Sims	RT(s)	Safe
[51,53]	[50,51]	[48,49]	6	5.7	✓
[49.51]	[45,46]	[51,52]	14	21	✓
[49.51]	[49.51]	[51,52]	27	76.2	X
[43,46]	[41,44]	[39,42]	24	40.6	✓

Range of pacemaker designs (LRI values) for which the required safety property is maintained and violated.
LRI, Delay1, Delay2: the range of values that LRI and delays of Delay can take,
Sims: number of simulations,
RT: running time in seconds.

Conclusion

- Simulation-based compositional verification can help improve reliability of medical devices
- Static analysis (IS-discrepancy) of only component-level is needed, which can be computed on-the-fly
- The technique can handle inter-component delay and is easily applicable to new topologies.

References

[1] Z. Huang, C. Fan, A. Mereacre, S. Mitra and M. Kwiatkowska. Simulation-based Verification of Implantable Medical Devices with Guaranteed Coverage. IEEE Test & Design, 2015
[2] Z. Huang, C. Fan, A. Mereacre, S. Mitra and M. Kwiatkowska. Invariant Verification of Nonlinear Hybrid Automata Networks of Cardiac Cells. CAV, 2015
[3] Z. Huang, C. Fan and S. Mitra. Bounded Invariant Verification for Time-Delayed Nonlinear Networked Dynamical Systems. IFAC NAHS, 2016

SCIENCE OF SECURITY
VIRTUAL ORGANIZATION
Funded by the National Security Agency.
INFORMATIONTRUST INSTITUTE