NSF:CPS:1035658, Exploratory Research: Safety-Oriented Hybrid Verification of Medical Robotics

Matthew Might, Ganesh Gopalakrishnan, John Hollerbach, Dennis Parker
University of Utah: School of Computing and Department of Radiology

Motivation and goal The whole-system design and modeling of complex medical robotics involves analog sensors and actuators; discrete software controllers; piecewise, non-linear, discontinuous biological tissues/media; and probabilistic human administrators.

In the best case, the failure of such systems risks limb. In the worst, life.

The goal of our project is to explore and investigate paradigms for the whole-system design, modeling and formal verification of cyber-physical-biological systems.

Motivating application To ground this project in practice, the motivating application is MRgHIFU: an MR-guided robotic surgeon wielding a high-frequency ultrasound as a scalpel for noninvasive surgical ablation of cancerous tissue. We selected this system because (1) it has clear humanitarian broader impacts, (2) it has demanding clinical safety requirements acting as a barrier to formal approval and clinical adoption, and (3) modeling and verification of the system and those requirements requires a complex synthesis of components with nonlinear behavior.

Research objectives Our specific research objective is the exploration and investigation of paradigms for the whole-system design, modeling and verification of cyber-physical-biological systems.

Scientific directions We are developing and investigating flow-driven-transducer networks as a paradigm for the design and modeling of cyber-physical-biological systems. Such networks formally model heterogenous systems with discrete, continuous and probabilistic components. Specific approaches being investigated include hybrid and timed automata, abstract-interpretive inference thereof and model-checking techniques for nonlinear differential equations.

Techniques and findings Findings to date include (1) a prototype core calculus for MATLAB—λ_M—to support analysis and modeling of high-level controllers; (2) a formal framework for flow-driven transducer networks; (3) abstract interpretive methods for hybrid specification synthesis; (4) probabilistic automata to model healthcare workers; and (5) characterizations of safety and liveness for cyber-physical-biological systems.

Keywords MRgHIFU, medical robotics, tumor ablation, hybrid systems, flow networks, model-checking, abstract interpretation, hybrid automata, formal verification