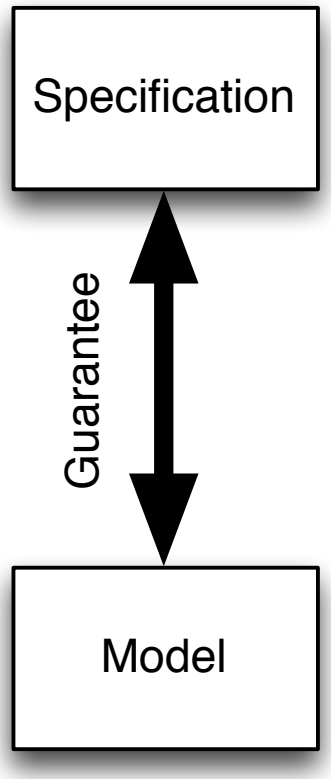
Towards Zero-Defect Surgical Robot Systems

Yanni Kouskoulas
Johns Hopkins University/APL

Feb 2014

Towards Building Zero-Defect Systems



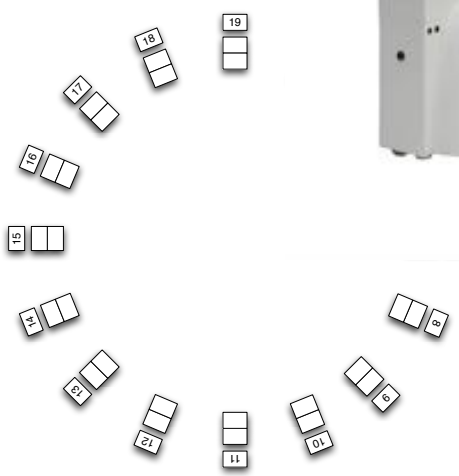
Description of system behavior.
What overall effect does the system have?

Logical argument that model behavior matches specification.

Description of system construction.
How are system components connected?

Prior Work Applying FM to Surgical Robots

- Applied formal methods to two separate surgical robot software components
- Found flaws, fixed them via redesign, proved that fixes worked, and that there were no more bugs
- Much more powerful than testing approaches

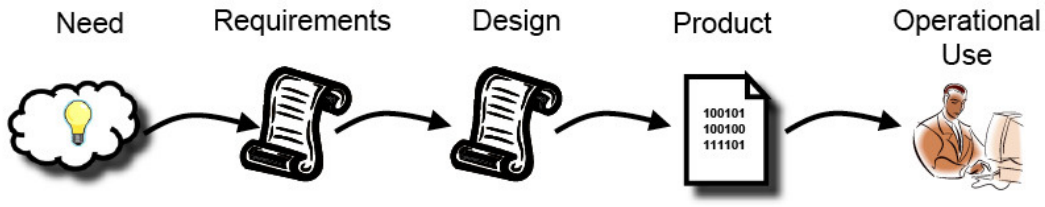


Prior Work Applying FM to Surgical Robots

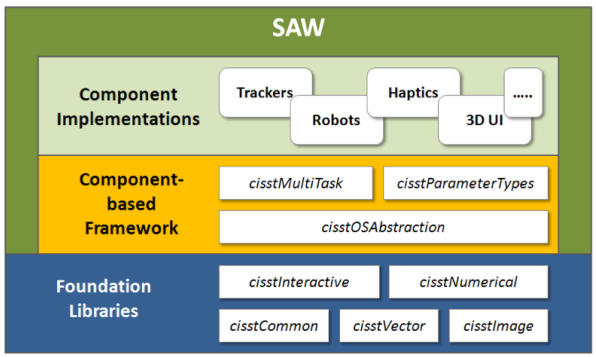
- Guaranteed fresh and uncorrupted data transfer by lock-free concurrent data exchange implementation
  - Surgical Assistant Workstation software library
  - Kazanzides, P., et. al. *Proving the correctness of concurrent robot software*, Proc. IEEE Intl. Conf. on Robotics and Automation (ICRA), pp.4718,4723, 14-18 May 2012
- Guaranteed safe enforcement of motion constraints by control algorithm when interacting with robot dynamics
  - Experimental skull-base surgery robot
  - Kouskoulas, Y, et al. *Certifying the safe design of a virtual fixture control algorithm for a surgical robot.* Proc. 16th Intl. Conf. on Hybrid systems: computation and control. ACM, 2013

Towards Building Zero-Defect Systems

- Different proofs for different development activities
  - Developmental guarantees ensure components implement correct functionality



  - Compositional guarantees help ensure existing components interact together to support higher-level objectives



Research Questions

Develop a framework that helps us create more comprehensive safety guarantees than are possible today

- How do we combine guarantees from different logics at different levels of abstraction into an algorithm for a single component?
  - Prove that control algorithm safely restricts movements in the presence of robot dynamics, but also that it provides data to other components through a standard interface
- How do we stitch together a web of detailed component guarantees to prove correct emergent system behavior?
  - Prove, e.g. "safe and accurate incisions, according to preoperative plan"
  - Component-level guarantees are treated as axioms for the proof about emergent behavior
  - Axioms not necessarily in the same language