Seventh Annual
Cyber-Physical Systems Principal Investigators' Meeting
Arlington, VA | October 31 – November 1, 2016

Towards Resiliency in Cyber-physical Systems for Robot-assisted Surgery

CNS 1545069; December 2015

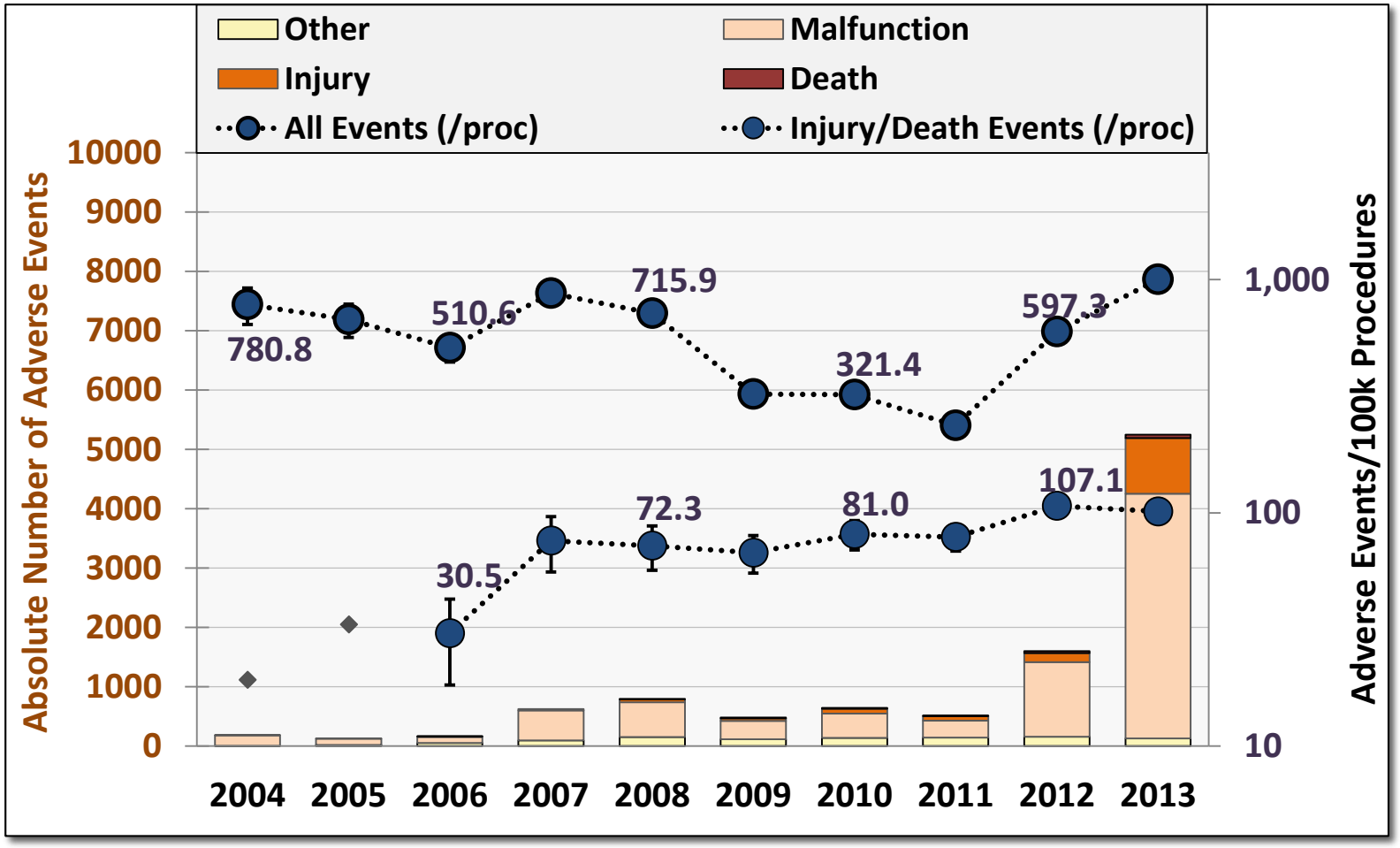
PI: **Ravishankar K. Iyer;**
Co-PIs: **Zbigniew T. Kalbarczyk, Thenkurussi Kesavadas**

Electrical and Computer Engineering
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign

Challenges

- Timely and accurate detection, prediction, and mitigation of incidents during robot-assisted surgery.
- An in-depth analysis of incident causes,
  - complex interactions among the system components, human operators, and patients
- Safety, reliability, and resiliency assessment of the robotic systems in the presence of realistic safety hazards, reliability failures, and malicious attacks
- Continuous monitoring for detection of safety, reliability, and security violations to enable timely recovery

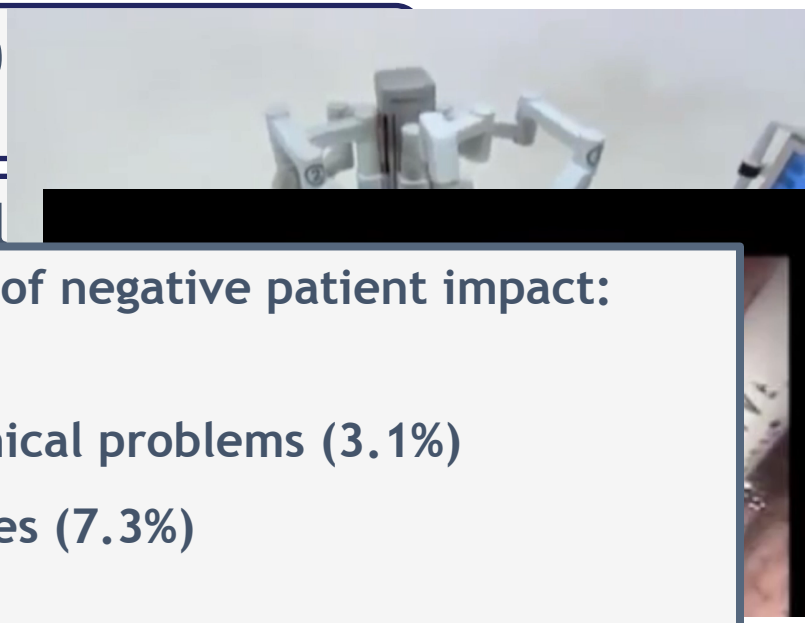
Safety Incidents in Robotic Surgery



Burnt/Broken pieces of instruments (14.7%):
- Falling into the patient's body, burning, and injury
- Interruption of procedure

Electrical arcing of instruments (10
- Burning of the tissues/organs under surgery

System errors. Video/imaging probl

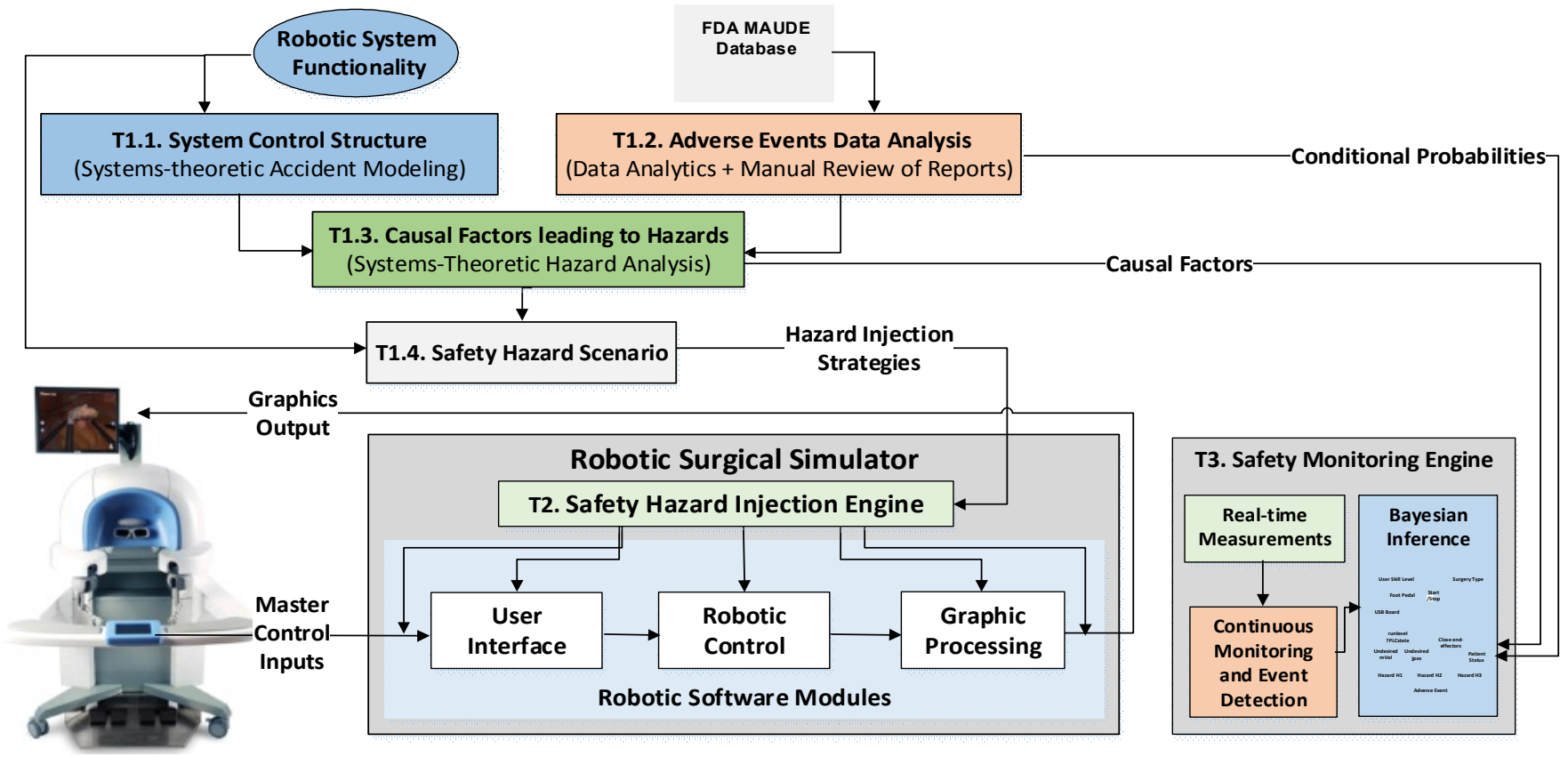


Given an adverse event, ~24% chance of negative patient impact:
- Injuries and deaths (14.4%)
- System resets to troubleshoot technical problems (3.1%)
- Conversion to non-robotic techniques (7.3%)
- Rescheduling the procedure (2.5%)

Approach

Framework components

- ***Robotic surgical simulator*** to model: behavior of human operators, dynamics of robotic hardware and tool-tissue dynamics.
- ***Safety hazard injection engine*** to assess resiliency
- ***Safety monitoring engine*** to detect and mitigate hazards



Scientific Impact

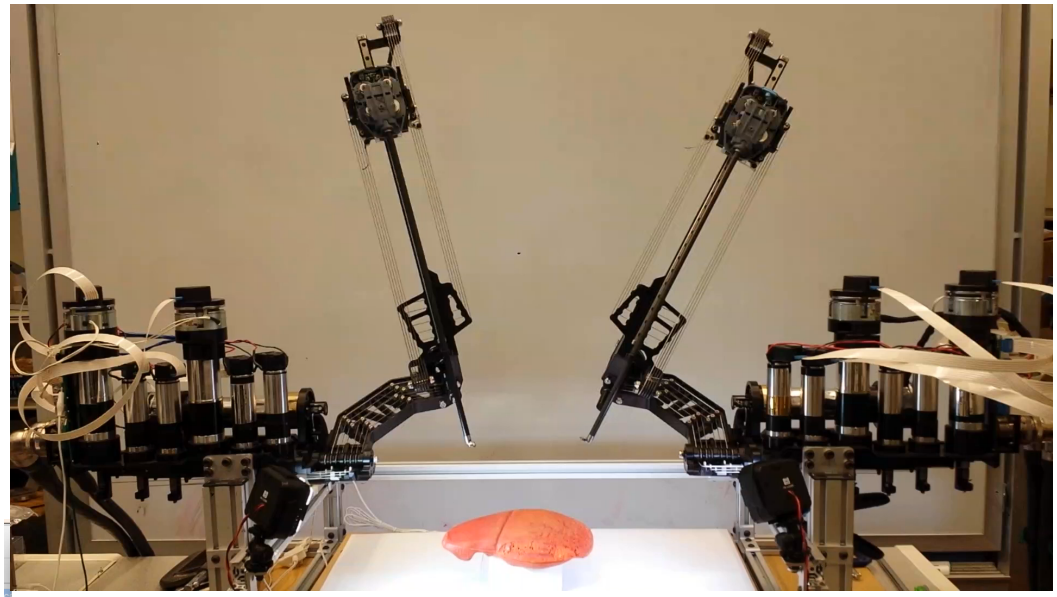
- Insights into understanding of resiliency problems that impact safety of the physical processes without introducing anomalies in the cyber domain.
- General principles for detecting cyber-physical attacks, which combines the knowledge of both cyber and physical domains.
- Demonstration of practicality of the approach in domains where CPS are the basis for delivering a service (e.g., transportation or electric power grids)

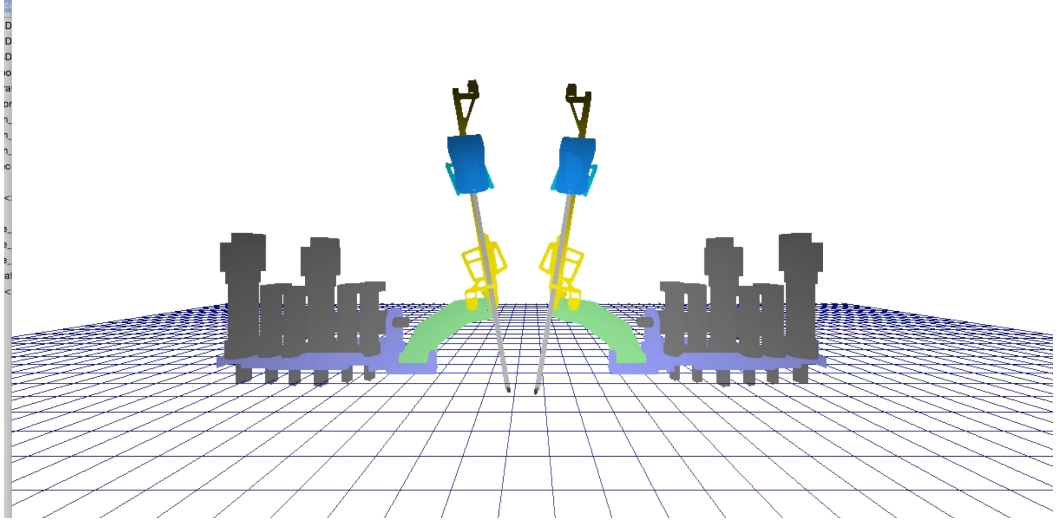
Broader Impact

- Strategy for design and assessment of a broad class of control cyber-physical systems, which involve human in on-line decision making loop.
- Provide industry with insights on safety and security issues in robot-assisted surgical systems (and beyond) and on how to improve the resiliency of future systems.
- Broadening participation in multi-disciplinary projects spanning medicine and engineering.
- Collaboration with academic institutions and industry partners to demonstrate the application of proposed analytics, validation techniques, and tools.

Safety Hazard Simulation

Safety Validation





Safety Training

Submitted to IROS 2016.