A Software Framework for Simulation of Safety Hazards in Robotic Surgical Systems

Homa Alemzadeh

In collaboration with:

Daniel Chen, Zbigniew Kalbarczyk, Ravi K. Iyer

Xiao Li , T (Kesh) Kesavadas

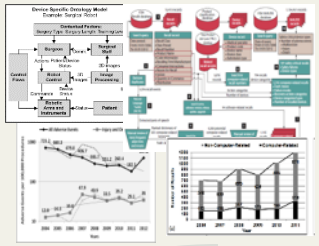
Coordinated Science Laboratory, UIUC

Jai Raman

Cardiac Surgery, Rush University Medical Center

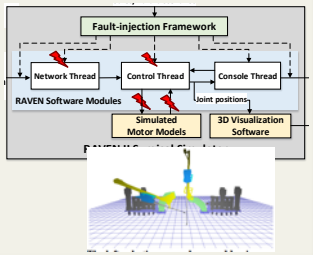
Analyzing Past Failures and Safety Incidents

- Real data on recalls and adverse events from the FDA
- Systems-theoretic accident models and hazard analysis



Evaluating System Resilience to Hazards

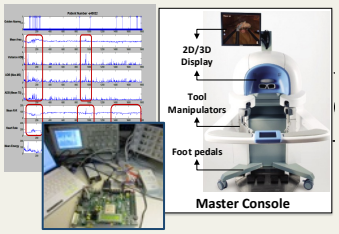
- Software fault-injection to emulate realistic failures
- Surgical simulators to recreate hazard scenarios



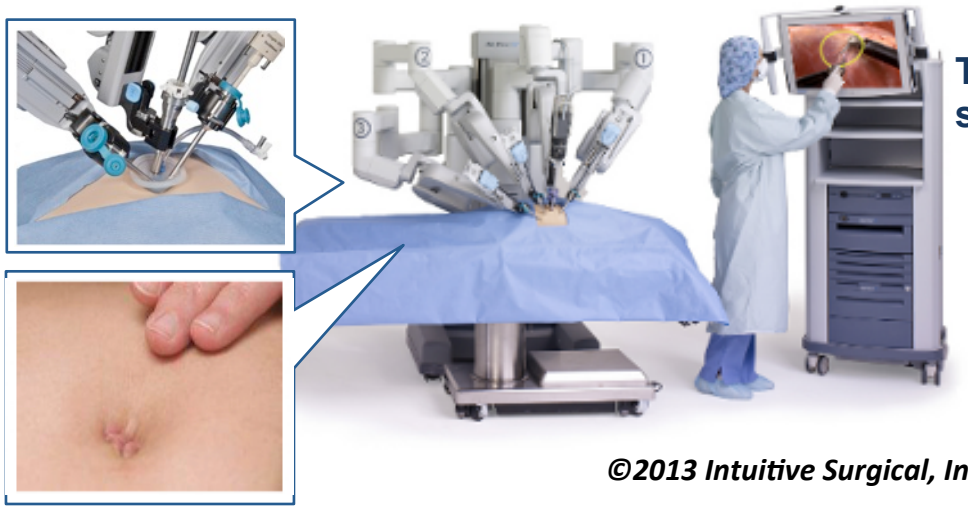
Safe and Resilient Robotic Surgical Systems

Design Resilient Surgical Systems and Simulators for Training

- Robust safety monitors for early detection and mitigation of safety hazards
- Advanced surgical simulators that prepare surgeons for handling safety-critical scenarios

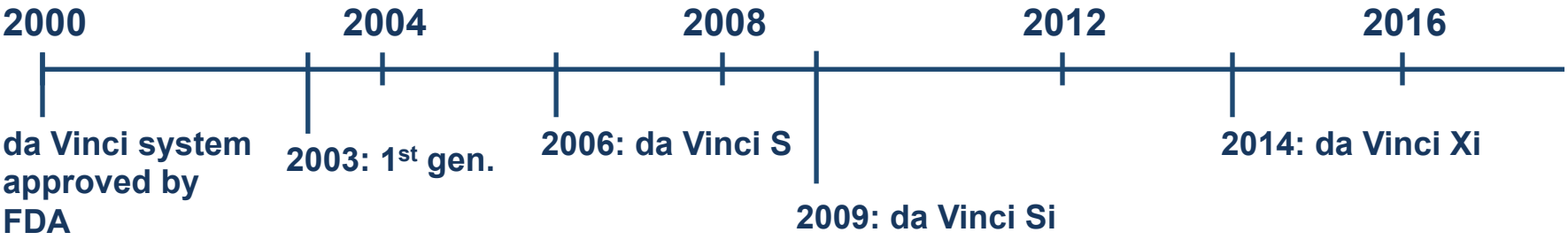


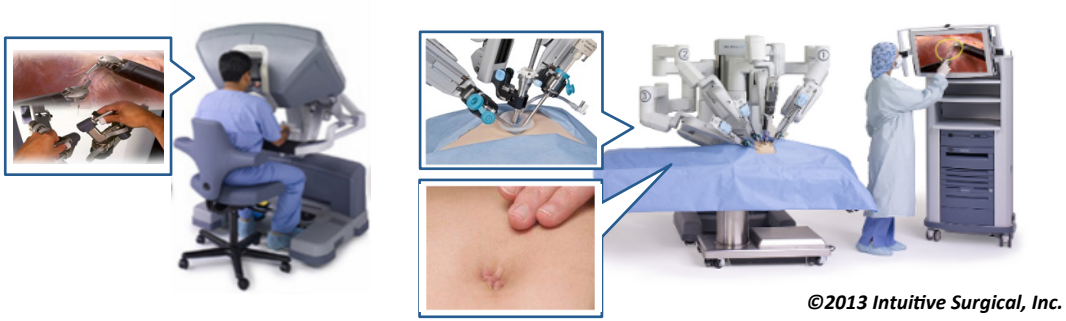
Robotic Surgical Systems



Tele-surgery

Robotic Surgical Systems





Robotic Surgical Systems

2000 — da Vinci system approved by FDA

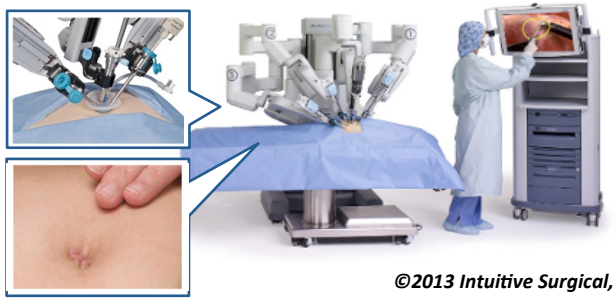
2004 — 2003: 1st gen.

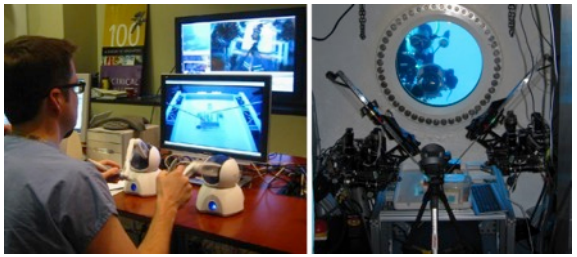
2008 — 2006: da Vinci S

2012 — 2009: da Vinci Si

2016 — 2014: da Vinci Xi

Tele-surgery



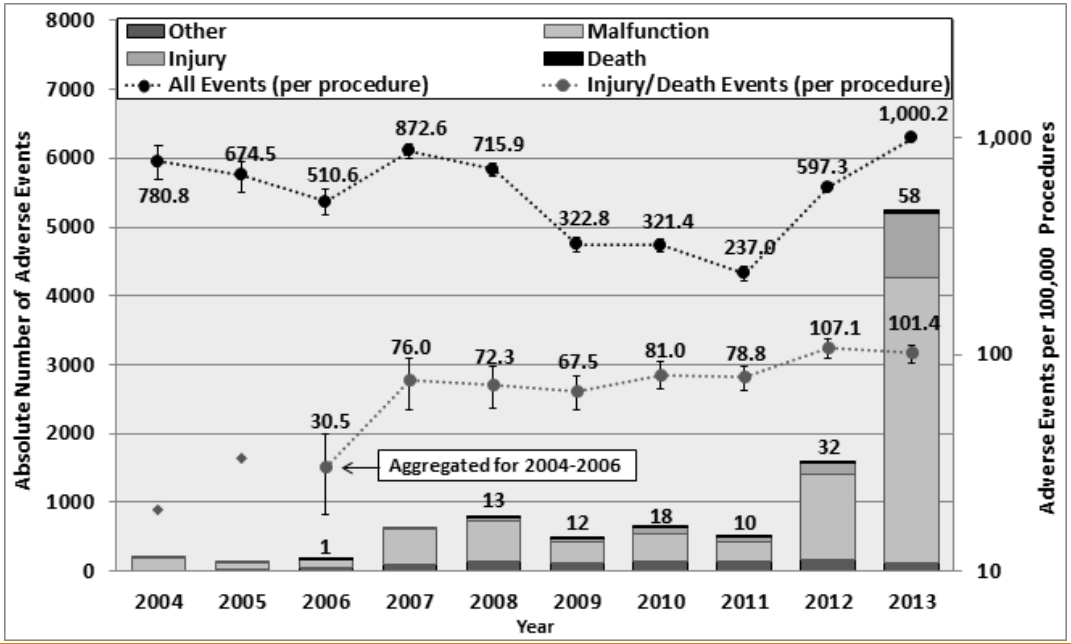


Surgeon in Seattle controlling Raven in Florida, 2007

Controlling a ZEUS robot in Strasbourg from New York, 2001

Adverse Events in Robotic Surgery

- 10,624 adverse events during **2000-2013**
  - 144 deaths and 1,391 injuries (14.4%)
  - 8,061 (75.9%) malfunctions

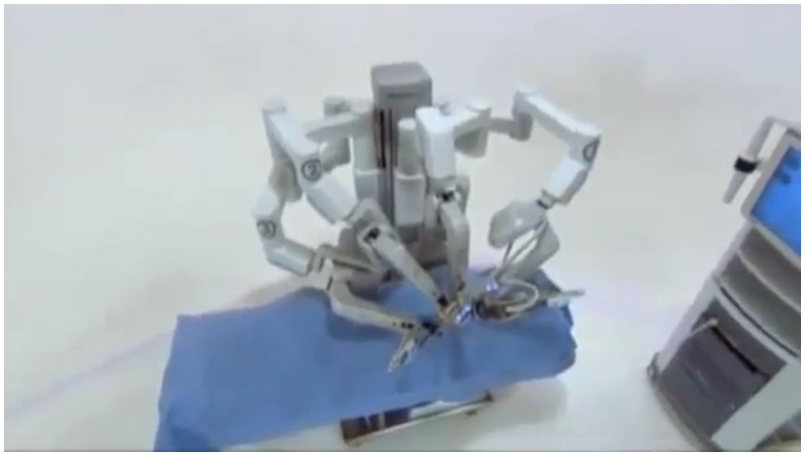


- An increase in reporting of adverse events, **32 times** since 2006
- Number of robotic procedures **increased 5 times**, since 2007.
- Rates of adverse events **per procedure** is relatively **constant**.

H. Alemzadeh, et al, Maxwell Chamberlain Memorial paper in The 50th Annual Meeting of the Society of Thoracic Surgeons, Jan. 2014.

Device Malfunctions and Patient Impacts

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



H. Alemzadeh, J. Raman, N. Leveson, and R. K. Iyer, "Safety Implications of Robotic Surgery: A Study of 13 Years of FDA Data on da Vinci Surgical Systems", Coordinated Science Laboratory, Technical Report UILU-ENG-13-2208, November 2013.

Device Malfunctions and Patient Impacts

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

Electrical arcing of instruments (10.5%):
- Burning of the tissues/organs under surgery

H. Alemzadeh, J. Raman, N. Leveson, and R. K. Iyer, "Safety Implications of Robotic Surgery: A Study of 13 Years of FDA Data on da Vinci Surgical Systems", Coordinated Science Laboratory, Technical Report UILU-ENG-13-2208, November 2013.

Device Malfunctions and Patient Impacts

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

Electrical arcing of instruments (10.5%):
- Burning of the tissues/organs under surgery

System errors, Video/imaging problems (7.6%)
- Interruption of procedure

H. Alemzadeh, J. Raman, N. Leveson, and R. K. Iyer, "Safety Implications of Robotic Surgery: A Study of 13 Years of FDA Data on da Vinci Surgical Systems", Coordinated Science Laboratory, Technical Report UILU-ENG-13-2208, November 2013.

Device Malfunctions and Patient Impacts

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

Electrical arcing of instruments (10.5%):
- Burning of the tissues/organs under surgery

System errors, Video/imaging problems (7.6%)
- Interruption of procedure

Unintended instrument operation (8.6%)
- Puncture/cut of organ under surgery

H. Alemzadeh, et al., "Safety Implications of Robotic Surgery: A Study of 13 Years of FDA Data on da Vinci Surgical Systems", Coordinated Science Laboratory, Technical Report UILU-ENG-13-2208, November 2013.

Device Malfunctions and Patient Impacts

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

Electrical arcing of instruments (10.5%):
- Burning of the tissues/organs under surgery

System errors, Video/imaging problems (7.6%)
- Interruption of procedure

Given an adverse event, about ~24% chance of negative impact on patients:

- **Patient injuries and deaths (14.4%)**
- **System resets to troubleshoot technical problems (3.1%)**
- **Conversion of procedure to non-robotic techniques (7.3%)**
- **Rescheduling of procedures to a later time (2.5%)**

H. Alemzadeh, J. Raman, N. Leveson, and R. K. Iyer, "Safety Implications of Robotic Surgery: A Study of 13 Years of FDA Data on da Vinci Surgical Systems", Coordinated Science Laboratory, Technical Report UILU-ENG-13-2208, November 2013.

Inadequate Operational Practices

- Inadequate handling of emergency situations
- Lack of training with specific system features
- Inadequate troubleshooting of technical problems
- Inadequate system/instrument checks before procedure
- Incorrect port placements
- Incorrect electro-cautery settings or cable connections
- Inadequate manipulation of robot master controls
- Inadequate hand and foot coordination by main surgeon
- Incorrect manipulation or exchange of instruments

From: FDA MAUDE Database; http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/Detail.CFM?MDRFOI__ID=1743065.

Inadequate Operational Practices

- Inadequate handling of emergency situations

INTUITIVE SURGICAL, INC. DA VINCI SURGICAL SYSTEM ENDOSCOPIC INSTRUMENT CONTROL SYSTEM Back to Search Results

Model Number IS1200 A4.3P9
Event Date 05/26/2010
Event Type Other
Manufacturer Narrative

The investigation conducted by the isi field service engineer (fse) concluded that system error code #20008 was associated with an input output distribution (iod) / remote interface adapter (ria) cable. The fse found a recessed pin at the connection end of the cable, preventing the cable from staying seated. The iod/ria cable is a bundle of wires which transmits power and sensor information between the surgeon side cart and the ria board associated with a particular slave arm. The system was repaired by replacing the affected ria cable. The system alarm (system generated fault code) functioned as designed and there was no injury to the patient. System error code #20008 appears when the da vinci safety system determines the angular position of one or more robotic joints on the specified manipulator, as measured by that joint's, primary control sensor (encoder) and the secondary sensor (potentiometer), are out of specified tolerance for agreement. Upon determining these conditions, the safety system puts da vinci in a "nonrecoverable safe state". As of (b)(4) 2010, there have been no reported recurrences of the issue at this hospital.

Event Description

It was reported that during a da vinci surgical procedure, the site experienced system error code #20008. An isi technical support engineer (tse) was contacted via telephone, who had the site reboot the system. The system was restarted with no issues and the planned procedure was successfully completed. The tse was contacted after the procedure, who informed the surgical staff that the system should not be used for another procedure as the system error code would likely return and become nonrecoverable. The site decided to proceed with their next scheduled da vinci surgical procedure and prior to using the system to perform any tasks, the site again experienced system error code #20008. The tse attempted to troubleshoot the issue and had the surgical staff power cycle and emergency power off the system multiple times, however, system error code #20008 continued to recur during homing. The patient had been under anesthesia for approximately 1 hour and 15 minutes when the surgeon made the decision to abort the planned procedure and reschedule it to a later date. No patient harm, adverse outcome or injury was reported.

From: FDA MAUDE Database; http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/Detail.CFM?MDRFOI__ID=1743065.

Safety Challenges

- **Accidents are under-reported and their causes are not well studied:**
  - Multi-dimensional analysis using system-theoretic causality models
  - Improved mechanisms for error logging and real time diagnosis
- **Monitoring and recovery mechanisms are passive:**
  - Reliability/Safety-driven design by considering the HW/SW interactions, physical system, and interactions between human operators and system
  - Safe real-time diagnosis and recovery from failures
- **Human operators are not trained for dealing with adverse events**
  - Proactive warnings and focused feedback on upcoming events and their corresponding troubleshooting procedures
  - Simulation-based training of surgical team by creating virtual safety hazard scenarios

Simulation of Safety Hazards

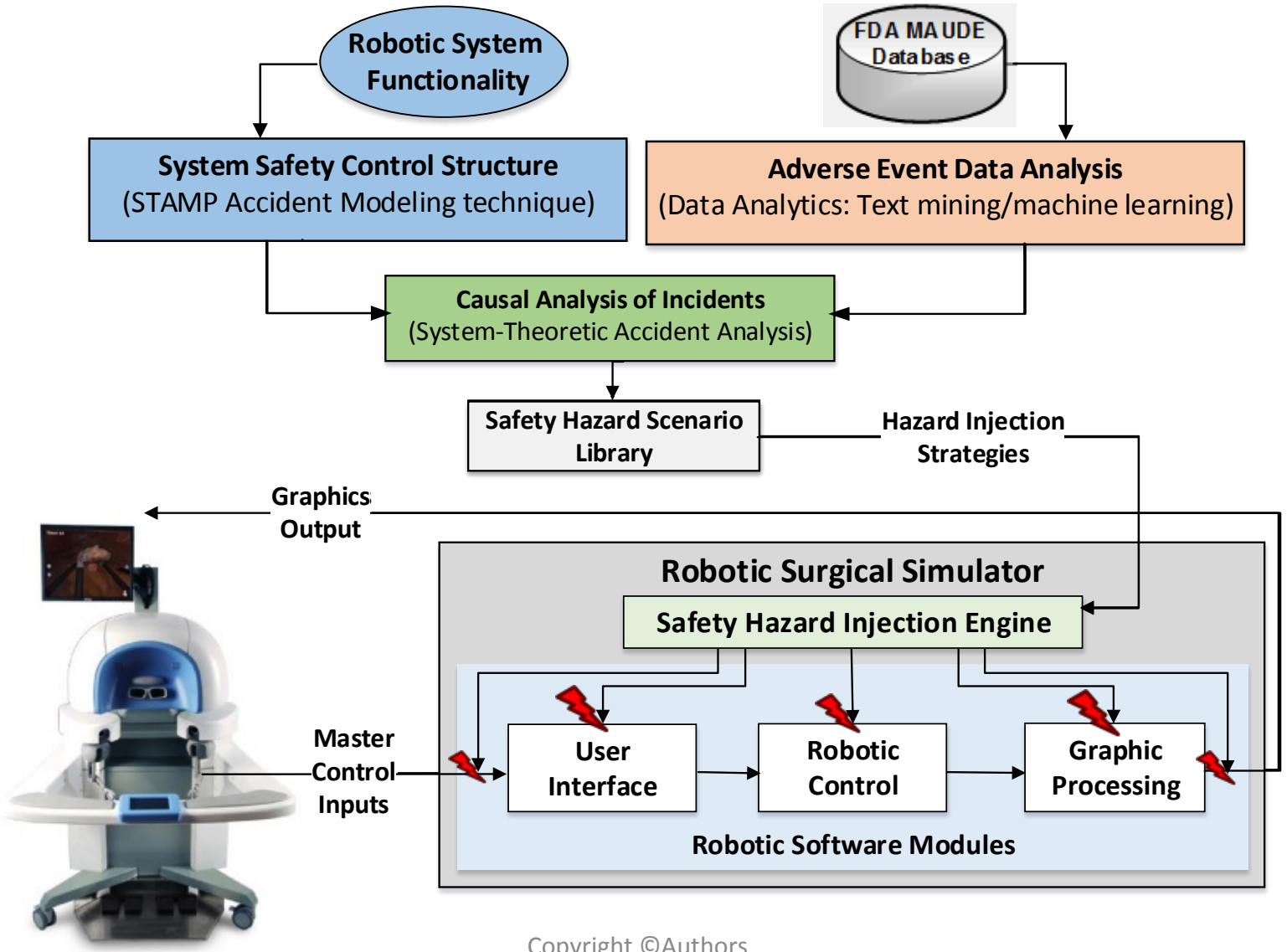
- To evaluate the safety and robustness of the next-generation of robotic surgical systems
- To develop and test safety monitoring and recovering mechanisms in design of robotic surgical systems

- To develop surgical simulators that prepare surgical trainees on how to deal with safety incidents

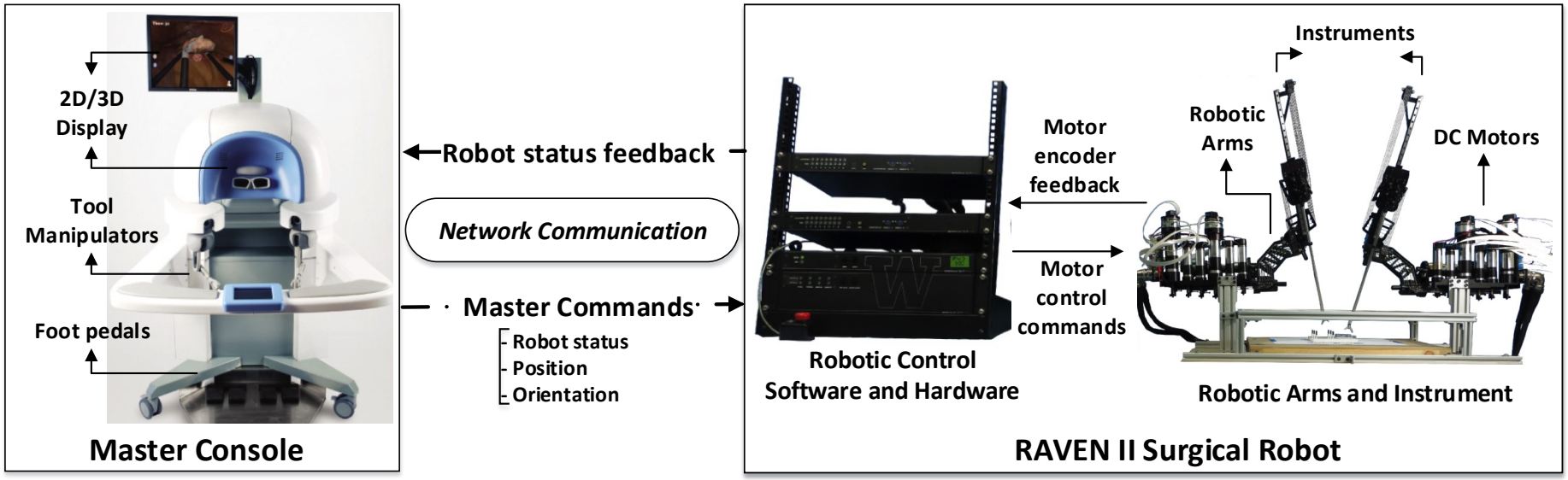
- **Augment the surgical simulators with fault-injection capabilities**
- **Simulate realistic safety hazard scenarios extracted from data**

H. Alemzadeh, Z. Kalbarczyk1, R. K. Iyer., T. Kesavadas, S. Small, J. Raman, "Simulation-based Training for Safety Incidents: Lessons from Analysis of Adverse Events in Robotic Surgical Systems," Presented at the *American College of Surgeons*' 8th Annual Meeting of the *Consortium of ACS-accredited Education Institutes*, March 2015.

System-theoretic Simulation of Safety Hazards

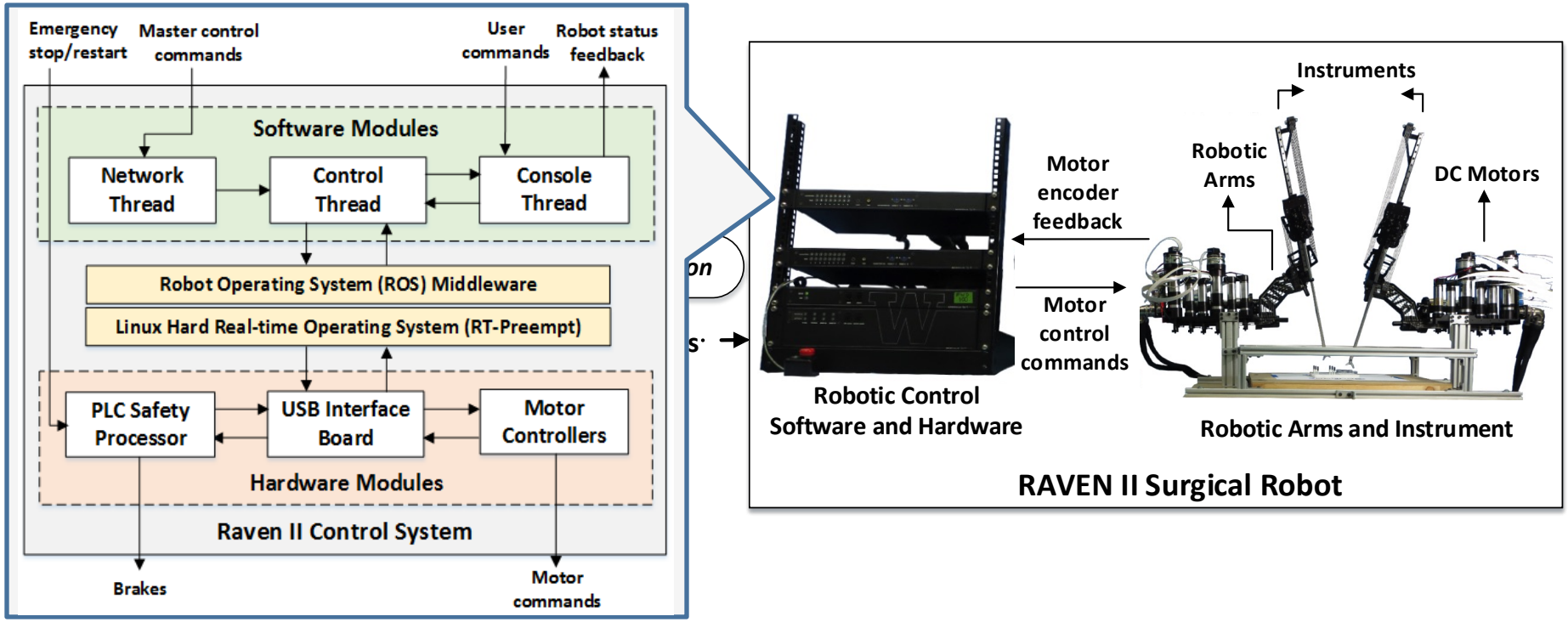


RAVEN II Robotic Tele-surgical System



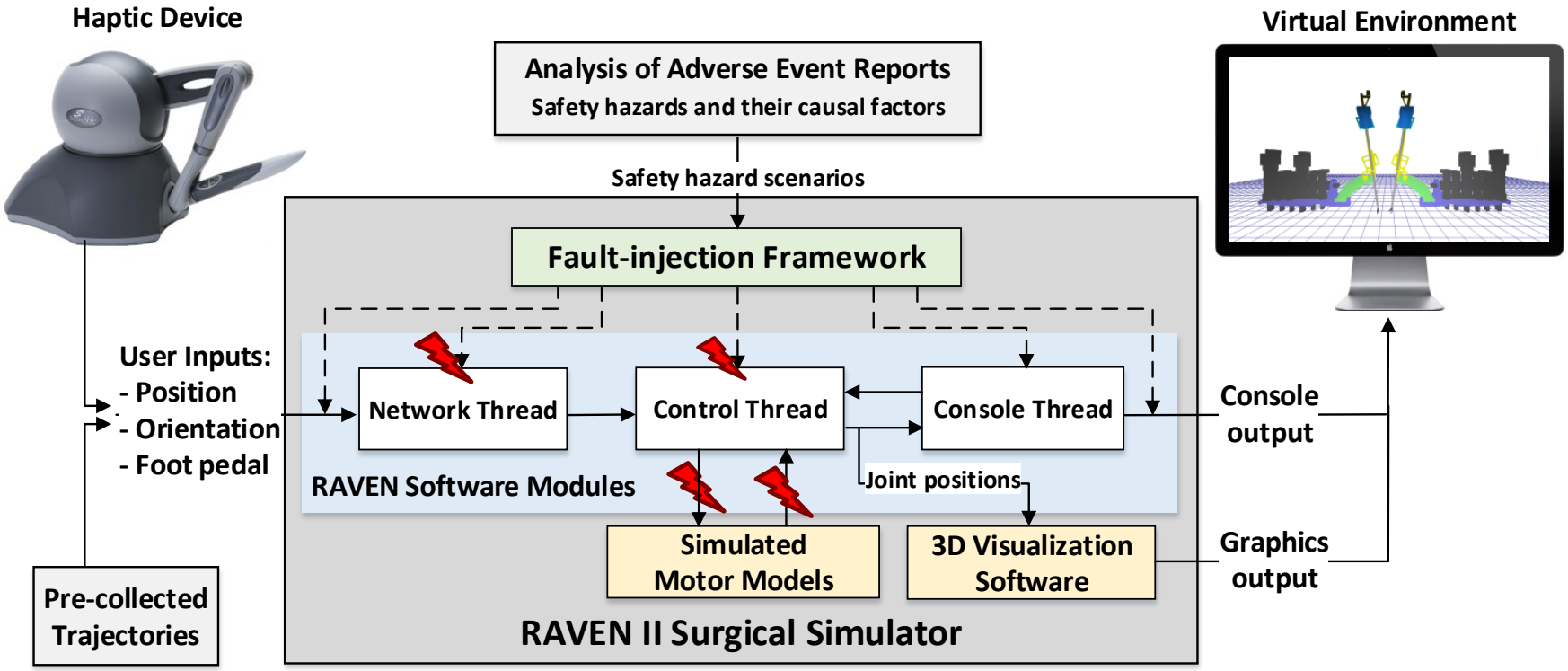
Applied Dexterity and Biorobotics Lab, University of Washington

RAVEN II Robotic Tele-surgical System



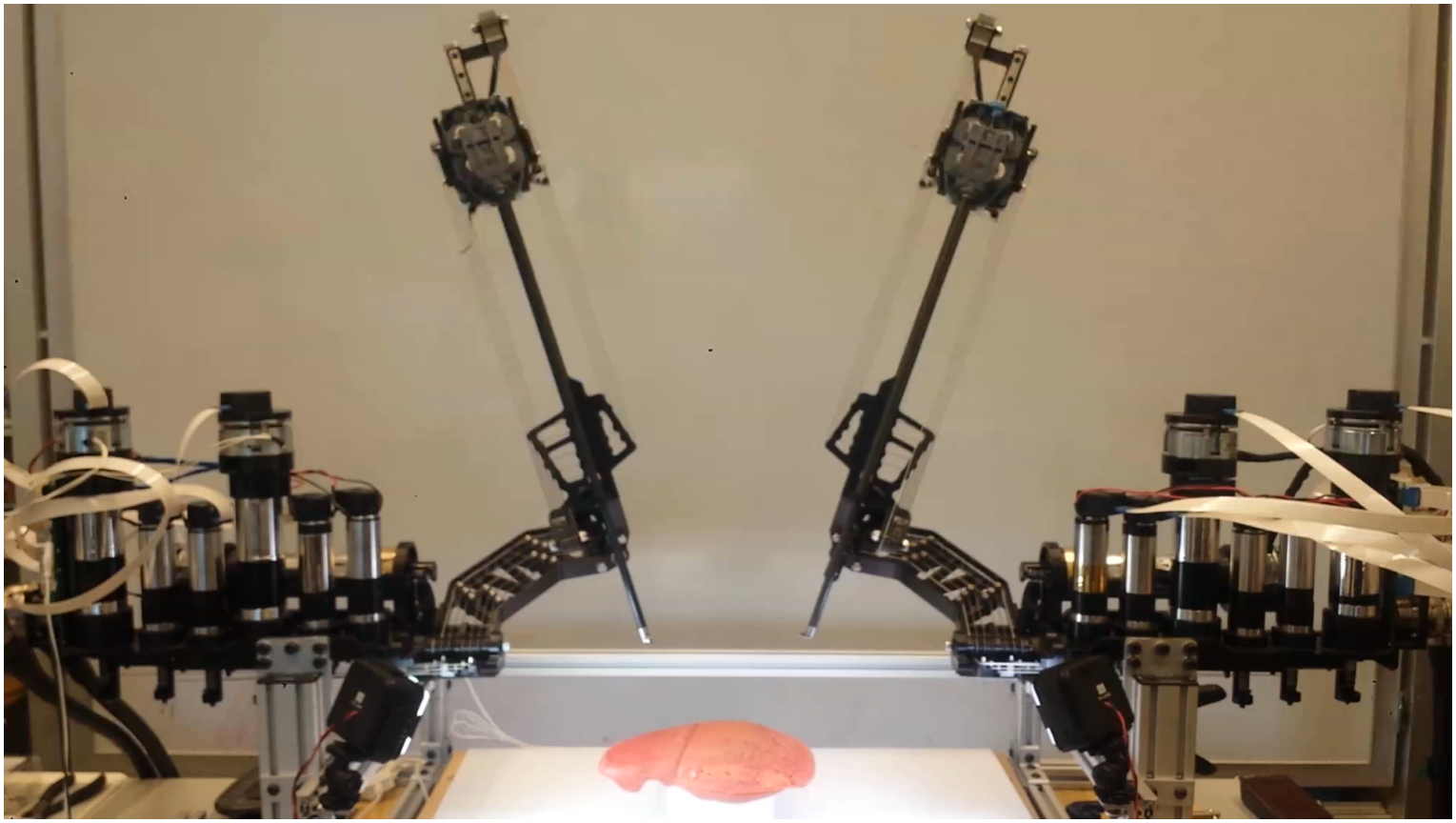
Applied Dexterity and Biorobotics Lab, University of Washington

RAVEN II Surgical Simulator + Software Fault-injection Framework



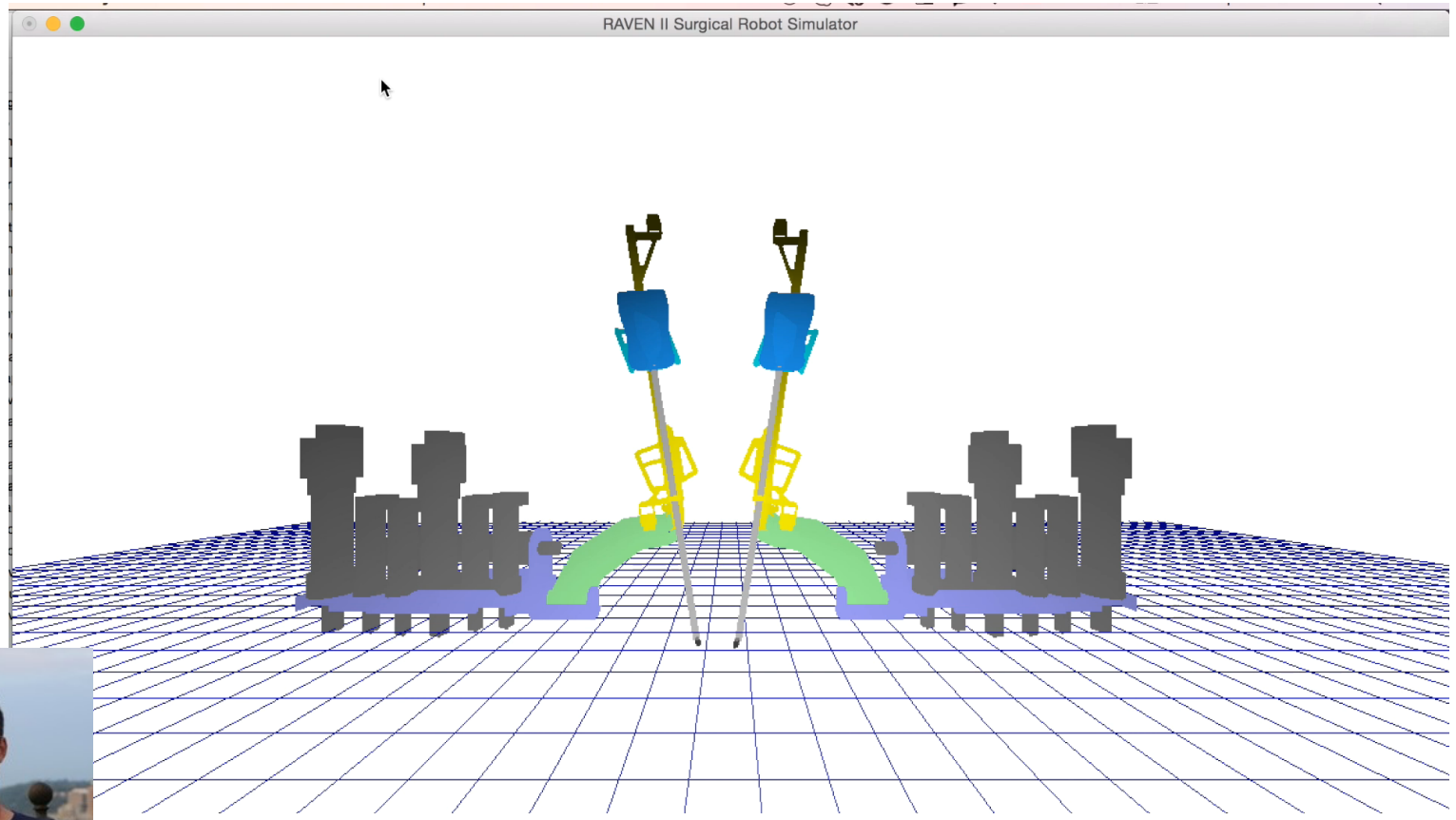
- Enables automated injection of realistic faults into RAVEN II control software
- Emulates realistic safety hazard scenarios extracted from the FDA Database

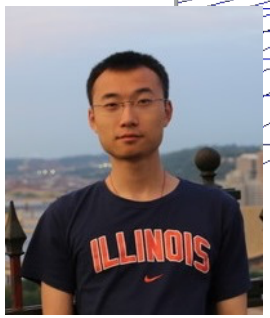
Running a Pre-collected Trajectory on RAVEN II Robot



Link to the video: https://www.dropbox.com/s/ylse2r6x4mduryz/Normal_Run.mp4?dl=0

RAVEN II Surgical Simulator

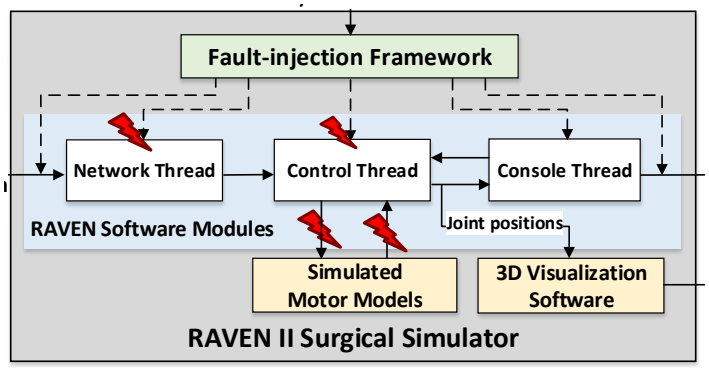


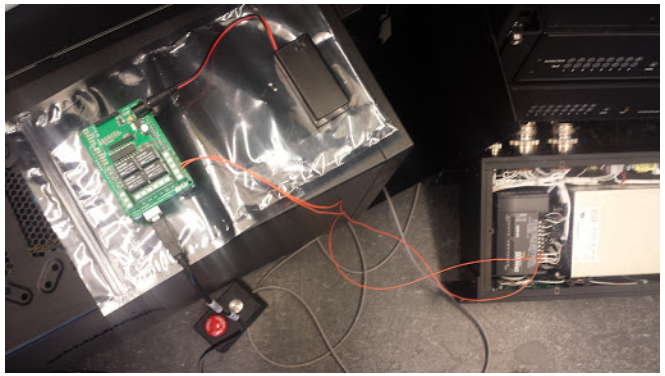


Xiao Li

Fault-injection Framework

- Targeted injection of causal factors in RAVEN II control software
  - Locations and types of faults and conditions under which they should be injected are defined based on STPA analysis + knowledge of software structure
  - Compile-time (code mutation) or run-time (breakpoint insertion)
- Works either in:
  - Simulated mode (for training surgeons)
  - The actual robot (for safety and security evaluation)
- Minimum modifications to RAVEN control software and hardware:
  - Software: Mechanisms for logging and visualization in virtual 3D environment
  - Hardware: Arduino Uno microcontroller added for automatic start and stop of PLC





Experiments on RAVEN II Simulator

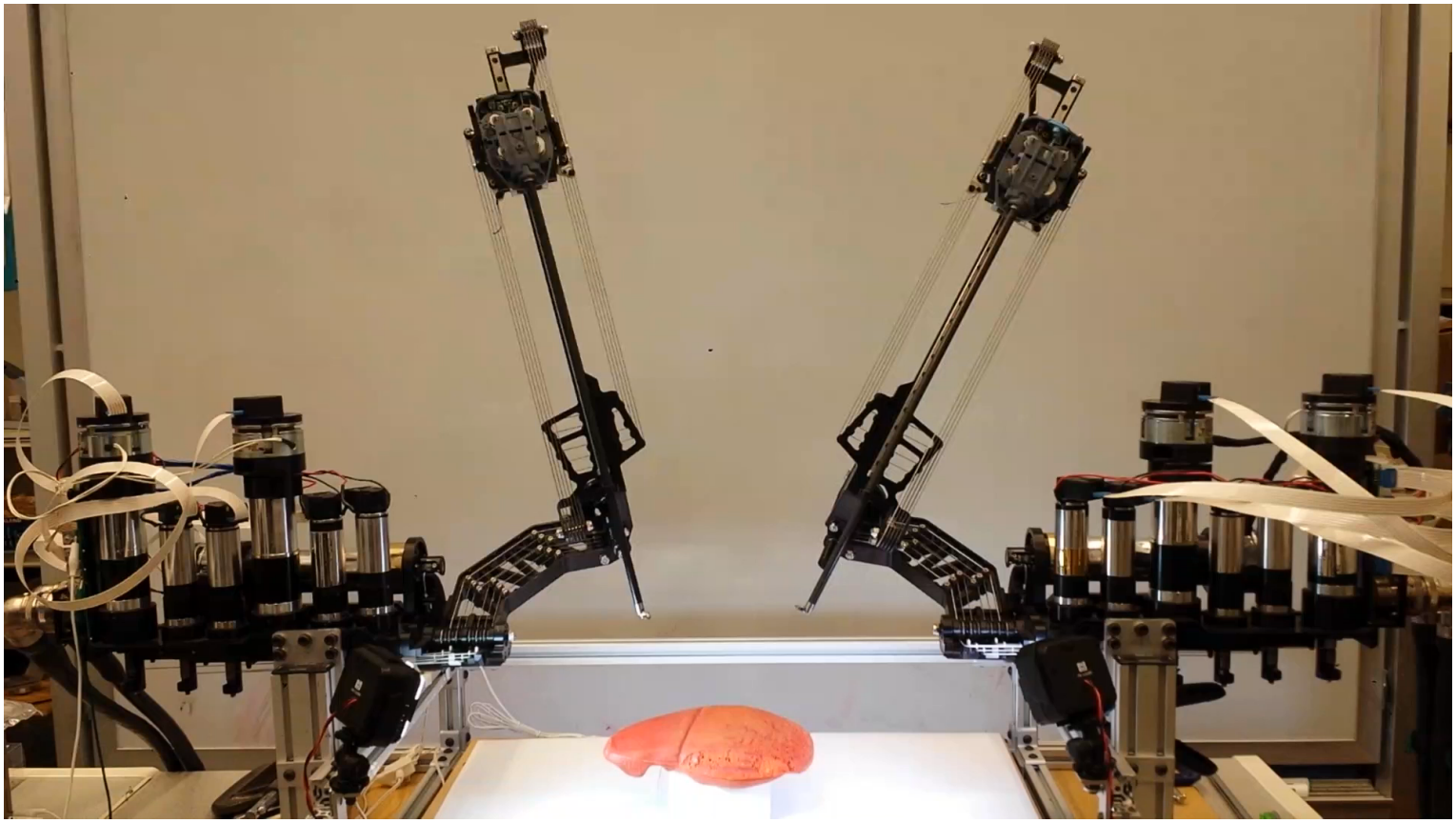
- Injected 5,500 faults into network and control threads on the simulator
- **Possible outcomes:**
  - Packet Dropped
  - IK Failure => E-STOP
  - Saturated to Joint Limits
  - Instrument (End-effectors) Collision Detected

- **Preliminary insights:**
  - Raven software is **robust against thread synchronization faults**.
  - Faulty user inputs (due to human error, manipulator failures, or software faults) cause **kinematics failures that either lead to E-stops or unintended jumps**.
  - **Majority of injections lead to software E-stop** which could be resolved by restarting the robot.
  - **Delay faults cause homing failure** and constant vibration of arms.
  - Faulty sensor readings cause saturation to joint limits.

Experiments on RAVEN II Robot

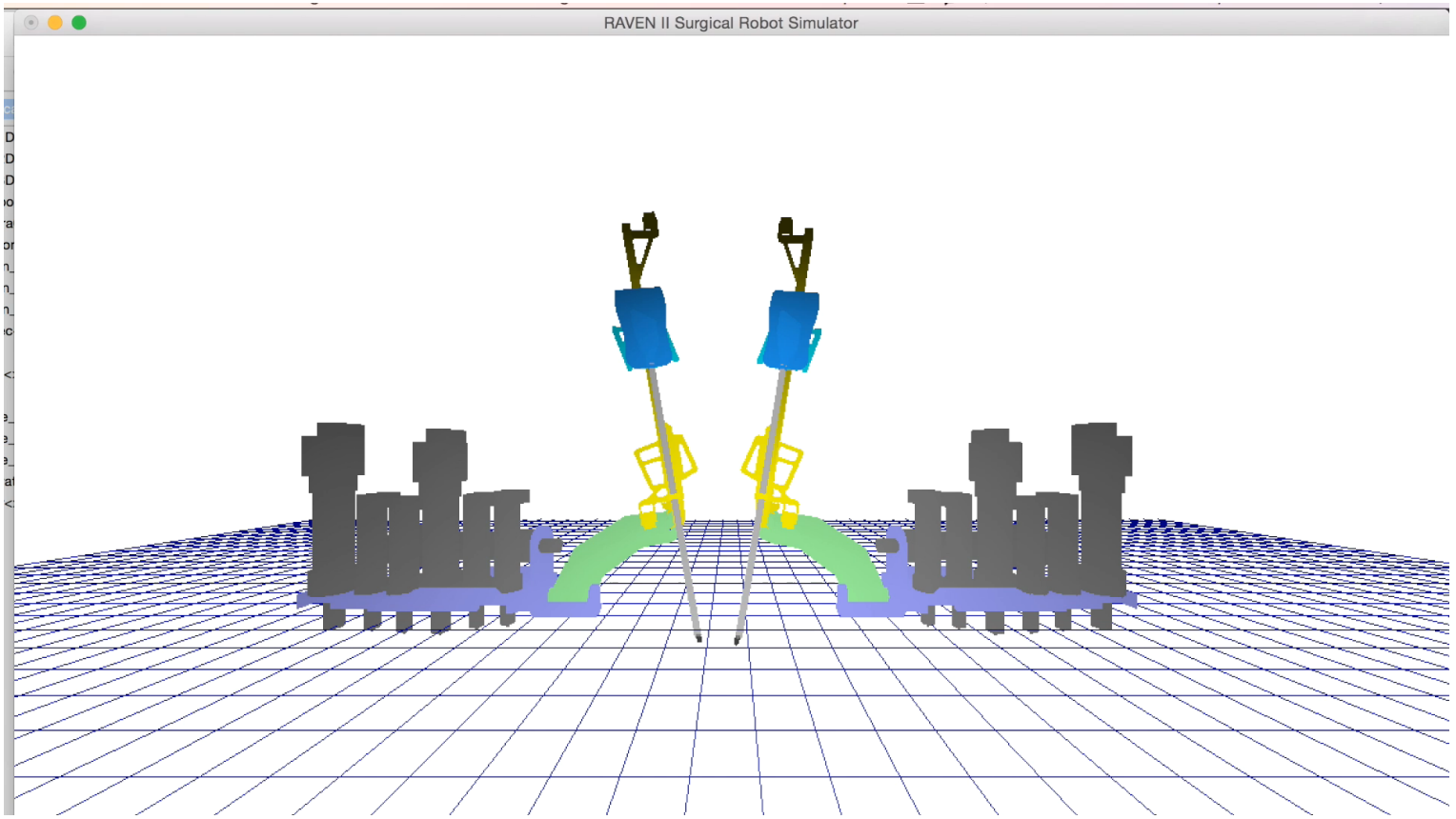
Safety Hazard Scenario	Possible Cause (Fault Type or Malicious Action)	Target Software Module	Target Variables	No. Manifested/ Injected Faults
Recoverable System Errors	Intermittent master tool manipulator malfunction *Corruption of user inputs by Man-in-the-middle (MITM) attack*	Network-Layer Thread	User-desired Position, Orientation, Grasper angle, Foot pedal	22/30
Non-recoverable System Errors	Sensor (encoder) malfunctions	Control Thread (*get_USB_packet*)	USB Board address or returned status	61/64
	Improper human operation or patient-side manipulator malfunction	Control Thread (*put_USB_packet*)	USB Board address or returned status	10/12
Unintended Instrument Movements (sudden jumps)	*Corruption of USB packets sent to hardware by getting unauthorized access to the OS or RAVEN software*		DAC commands sent to robotic joints	3/4*

Sudden Jump Simulated on RAVEN II Robot



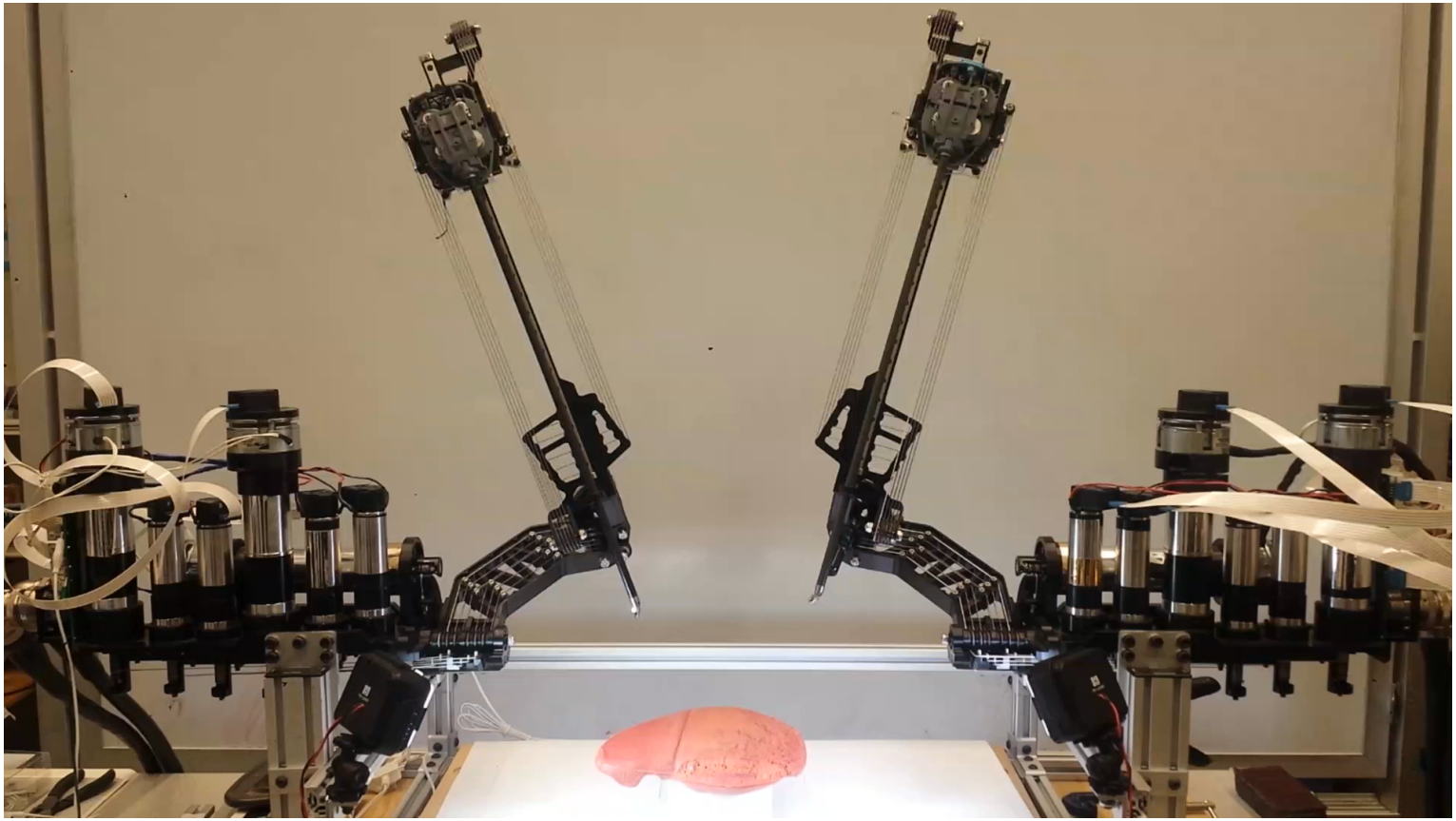
Link to the video: https://www.dropbox.com/s/rrx6f74xful38on/Sudden_Jump.mp4?dl=0

Sudden Jump Simulated on RAVEN II Simulator



Link to the video: https://www.dropbox.com/s/4zzejruob63stli/Simulator_Sudden_Jump.mp4?dl=0

Non-recoverable System Error Simulated on RAVEN II Robot



Link to the video: https://www.dropbox.com/s/0wa9evgwfj9nr6k/Repeated_Homing.mp4?dl=0

Our special thanks to Andrew Lewis, David Drajeske, and Blake Hannaford from Applied Dexterity and researchers at the University of Washington Biorobotics Lab for providing the open-source code for the RAVEN II surgical robot and allowing us to perform experiments on a RAVEN robot in their lab.

Thank You