

# Carter PhD Dissertation Award in Dependability

to recognize an individual who has made significant contribution to the field of dependable computing through his/her PhD dissertation research

Co-sponsored by:

- IEEE TC on Dependable Computing and Fault Tolerance
- IFIP Working Group on Dependable Computing and Fault Tolerance

## Evaluation Committee in 2017:

Christof Fetzer, Chair

Valeria Bertacco; Elmoottazbellah (Mootaz) N. Elnozabhy; Michael R. Lyu; Richard Schlichting

**15 Applications received**

Winner:

**HOMA ALEMZADEH**

with the thesis

**DATA-DRIVEN RESILIENCY ASSESSMENT OF MEDICAL CYBER-PHYSICAL SYSTEMS**

# Data-driven Resiliency Assessment of Medical Cyber-physical Systems

Homa Alemzadeh

Ph.D., University of Illinois at Urbana-Champaign, 2016

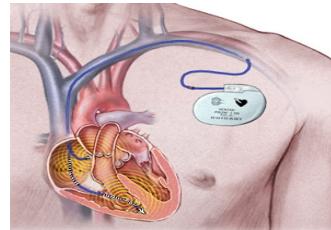
Advisors: Ravi Iyer and Zbigniew Kalbarczyk

[alemzadeh@virginia.edu](mailto:alemzadeh@virginia.edu)



# Medical Cyber-Physical Systems

Pacemakers



Insulin Pumps



Wearable Monitors



Patient Monitors



Infusion Pumps



Defibrillators



Surgical Robots



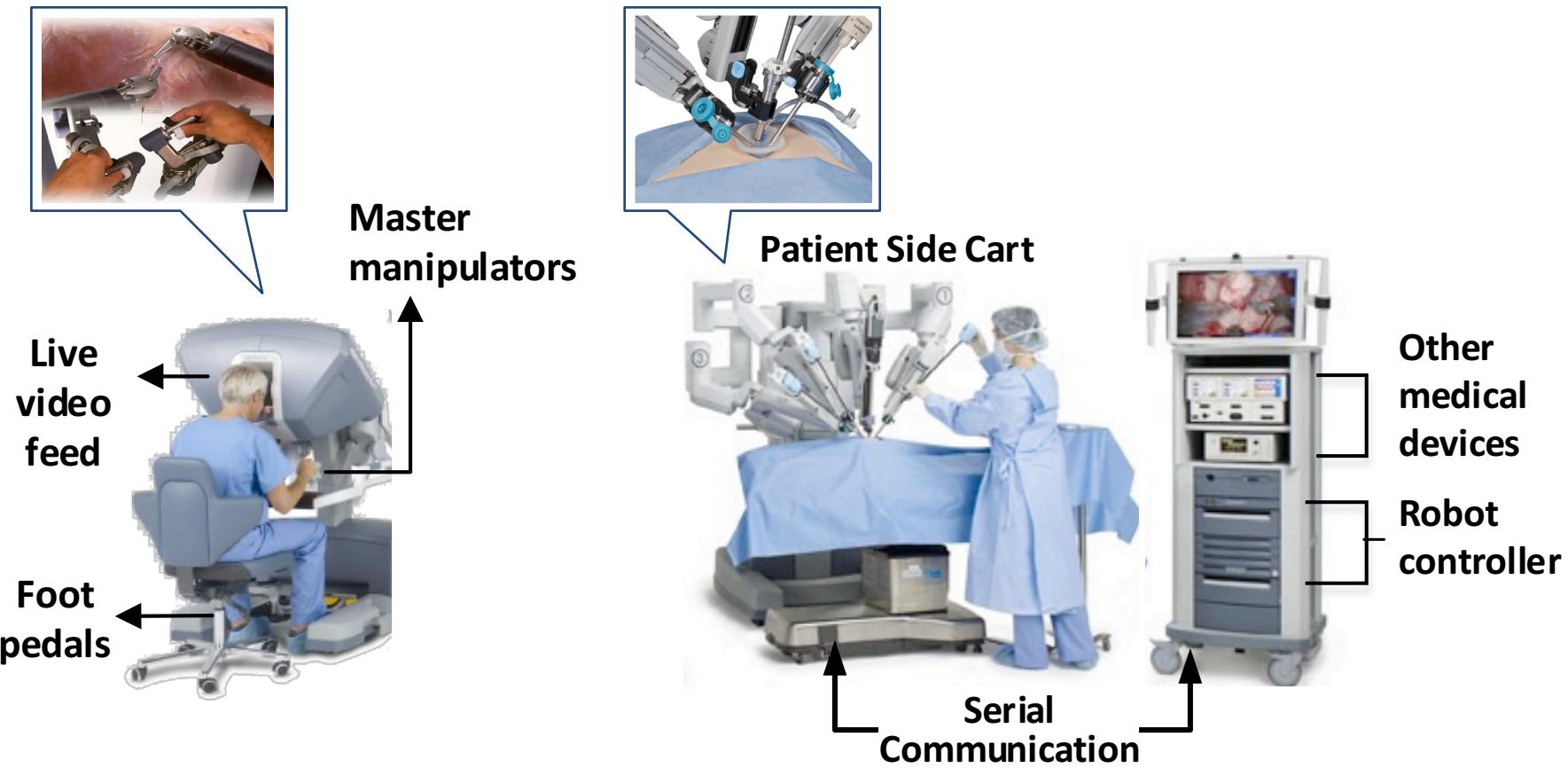
Imaging Systems



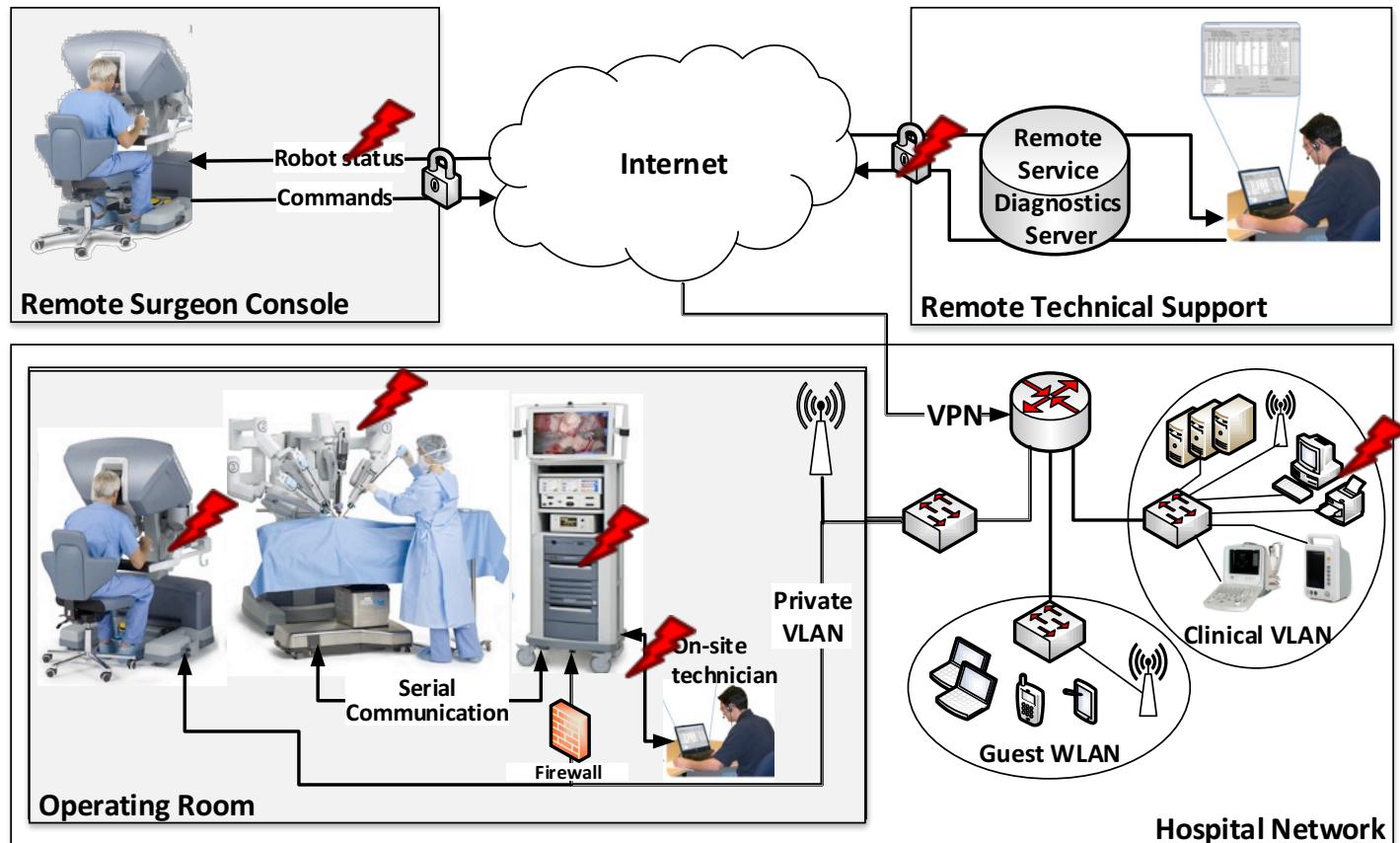
Linear Accelerators



# Human-Cyber-Physical Systems



# Human-Cyber-Physical Systems



# Catastrophic Events

## Accidental Failures

### GE Healthcare - Telemetry Monitoring Systems

Did not recognize a patient's telemetry rhythm.

Did not alarm a series of ventricular fibrillation events.

Patient Outcome: Death

FDA Adverse Event Report - 2010



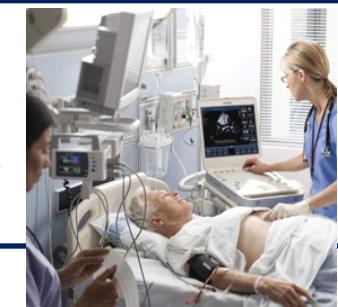
## Malicious Attacks

### Philips Medical Systems – XCELERA Imaging System

Due to a virus infecting several computers at a hospital, the XCELERA software could not be used from time to time.

Potential Patient Outcome: Death, health deterioration

FDA Adverse Event Report - 2009



- Over 17,000 recalls, more than 18 million devices
- 2.4 million adverse events, 923K injuries, 49K deaths

U.S. FDA, 2006-2013

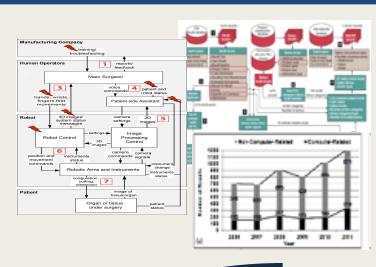
# Safety Challenges

- Causes and impacts of incidents not well studied
  - Causal analysis: HW/SW interactions, physical system dynamics, humans in the loop, and context
- Safety mechanisms not rigorously validated
  - Assessing resiliency against realistic safety hazards
- Passive monitoring and recovery mechanisms
  - Real-time detection and mitigation of system hazards
- System operators not well trained for incidents
  - Safety training by hazard simulation



## Analyzing Data on Past Safety Incidents

- Automated analysis of incident reports
- Systems-theoretic causality modeling



*IEEE Security & Privacy, 2013*

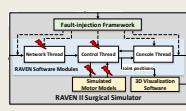
*IEEE CBMS, 2014*

*STS, 2014 (Memorial Paper)*

*PLOS ONE, 2016*

## Assessing Resilience to Safety Hazards

- Hazard analysis to identify causes for unsafe scenarios
- Software fault-injection to create realistic hazards



*ACS Meeting, 2015*

*Medical CPS, 2015*

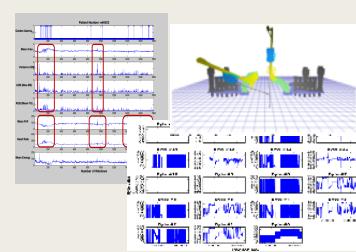
*SafeComp, 2015*

*IROS, 2016*

## Resilient Medical Cyber-Physical Systems

### Designing Resilient Systems

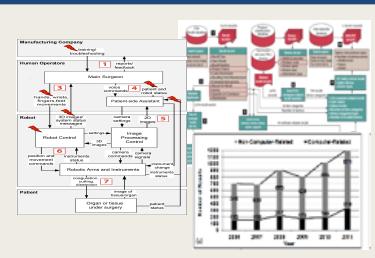
- Real-time detection and mitigation of safety hazards
- Safety validation in presence of accidental failures or malicious attacks



*IEEE DSN, 2016*  
*HotSoS, 2016*

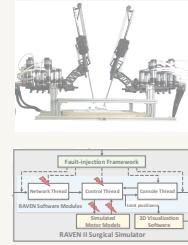
## Analyzing Data on Past Safety Incidents

- Automated analysis of incident reports
- Systems-theoretic causality modeling



## Assessing Resilience to Safety Hazards

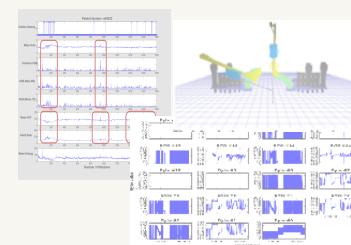
- Hazard analysis to identify causes for unsafe scenarios
- Software fault-injection to create realistic hazards



## Resilient Medical Cyber-Physical Systems

### Designing Resilient Systems

- Real-time detection and mitigation of safety hazards
- Safety validation in presence of accidental failures or malicious attacks



# Medical Device Incidents

## U.S. Food and Drug Administration (FDA)

**Recalls:** actions to correct/remove defective devices

Recalling Firm/ Manufacturer	GE Healthcare, LLC 3000 N Grandview Blvd Waukesha, Wisconsin 53188-1615
---------------------------------	---

Consumer Instructions Contact the recalling firm for information

Reason for Recall Transport Pro Monitor stops communication with the CARESCAPE Patient Data Module (PDM) after 414 days of continuous run time. This time will equate to different amounts of real time depending on how much the units is actually in service per day. Transport Pro contains an internal timer that is used to control the software and remind users to perform preventive maintenance. When this internal timer

Action GE Healthcare issued an "Urgent Medical Device Correction" letter dated September 17, 2010 to consignees. The letter was addressed to Hospital Administrator, Head of Biomedical Engineering and Nursing Manager. The letter described the product, Safety Issue, Affected Product Details, Safety Instructions Product Correction and Contact Information. Service representatives will update all of the affected Transport Pros with PDM that were distributed. Customers may contact GE at 262-548-2731 about this correction.

Quantity in Commerce 3266

Structured

Unstructured

**Adverse Events:** deaths, serious injuries, and malfunction reports

GE HEALTHCARE APEX PRO FH TELEMETRY SYSTEM TELEMETRY MONITORING SYSTEM

Event Date 12/20/2009

Event Type Death Patient Outcome Death

Event Description

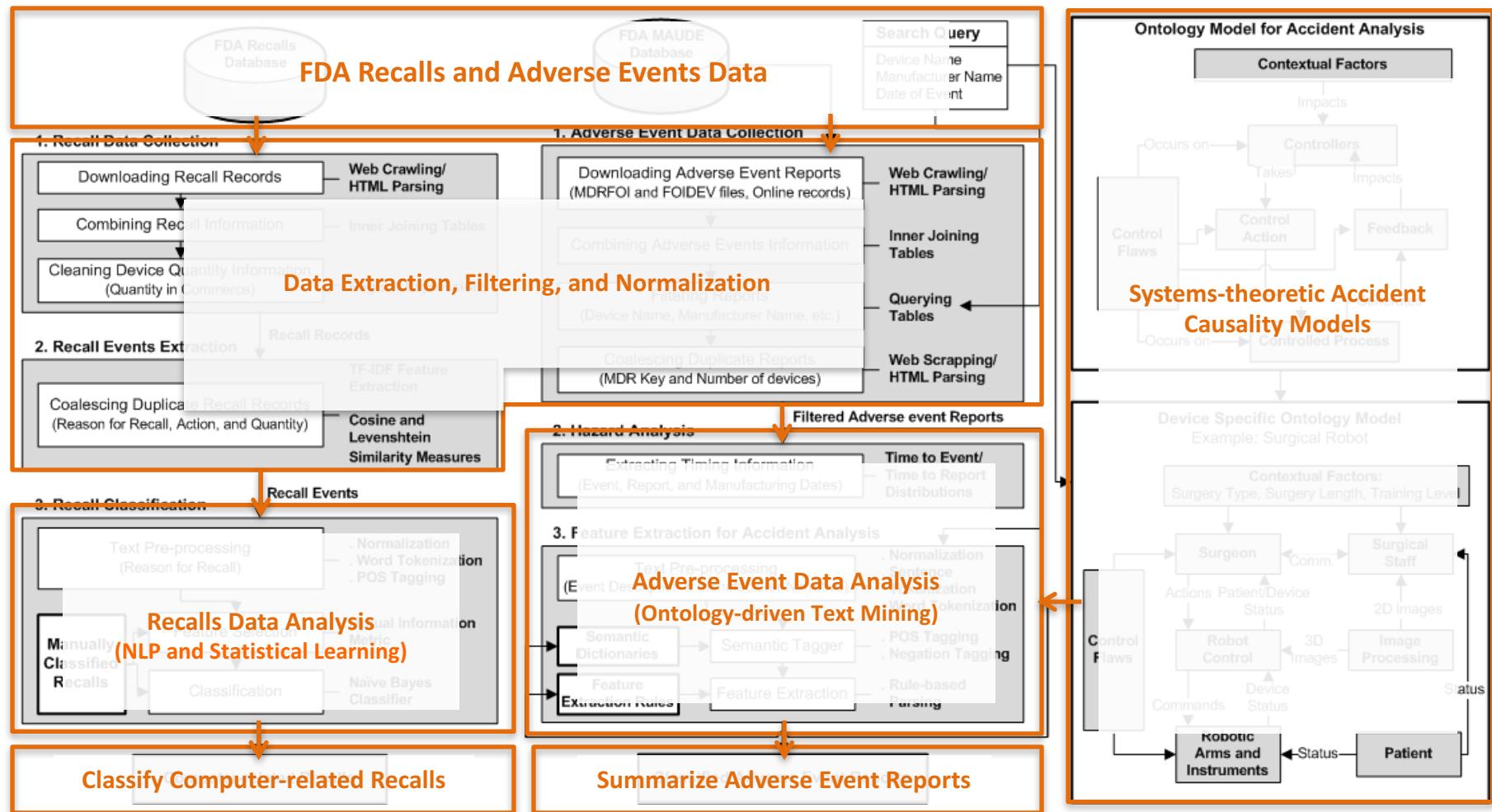
A customer reported that the apex pro telemetry monitor was not recognizing a pt's telemetry and the telemetry box were subsequently changed. An hour later, the pt experienced a series of fibrillation events; however, the monitor allegedly did not alarm. The pt reportedly coded a

Manufacturer Narrative

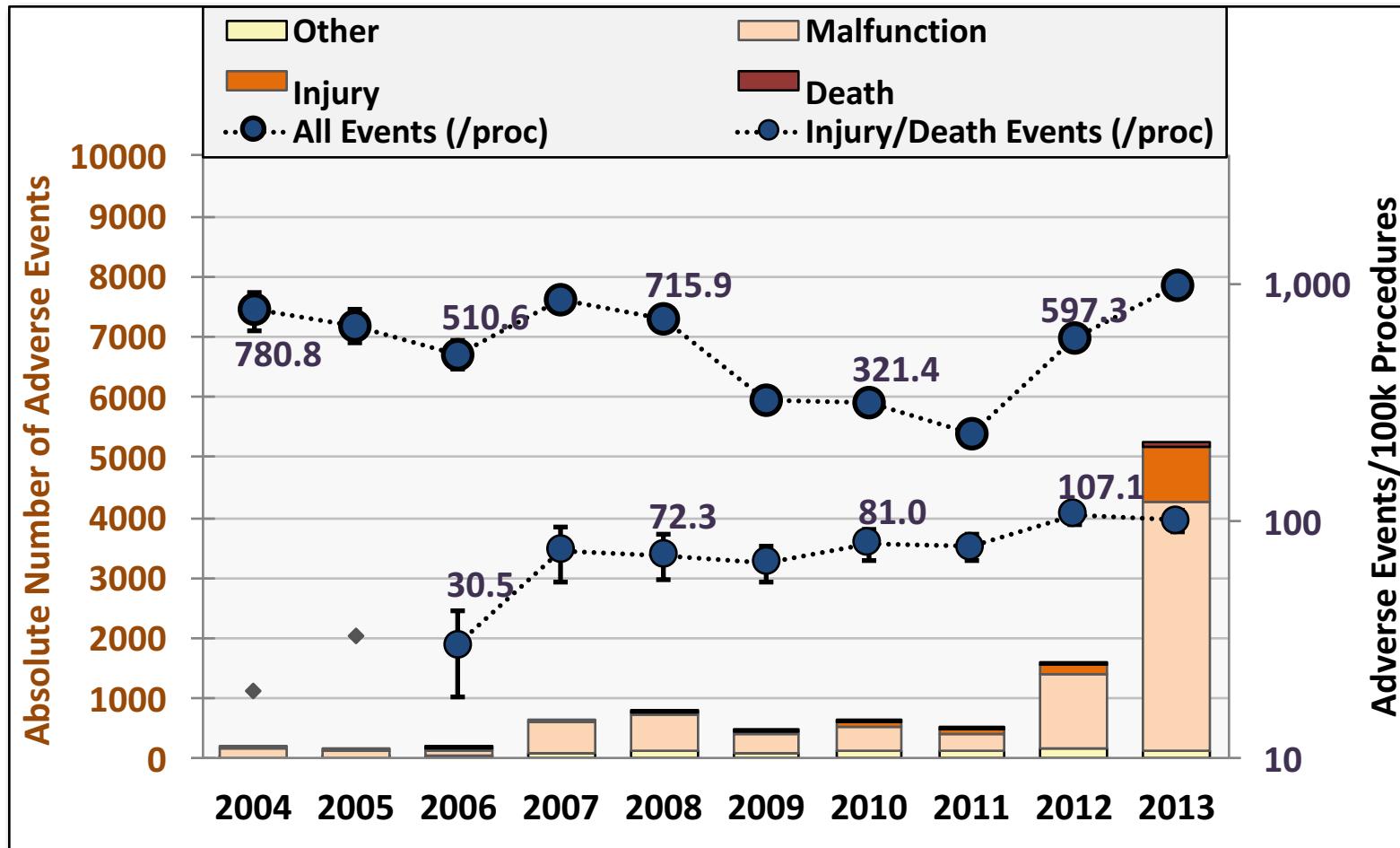
GE healthcare's evaluated the log files and graph strips provided by the customer. The telemetry box announced a vfib (ventricular fibrillation) at the time in question, which is consistent with the customer. The cic (central station); however, did announce audible and visually a number of events including multiple pause and brady events. These were announced at a warning level at the maximum volume of the system. There were no clinical operator interactions between 22:09:15 and 22:29:57. The next action performed was to silence the sounding cic around the ecg data that was provided suggests that there was insufficient best amplitude to have all

Structured  
Unstructured

# MedSafe



# Safety Incidents in Robotic Surgery



*Featured in Wall Street Journal, MIT Technology Review, BBC, NBC News, Gizmodo, among others.*

# 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

# 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

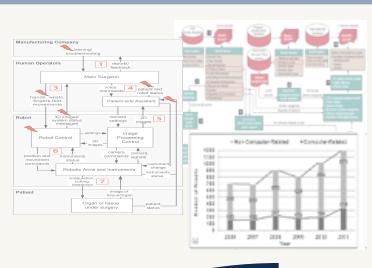
## System errors, Video/imaging problems (7.6%)

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%)

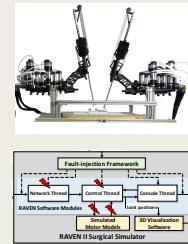
## Analyzing Data on Past Safety Incidents

- Automated analysis of incident reports
- Systems-theoretic causality modeling



## Assessing Resilience to Safety Hazards

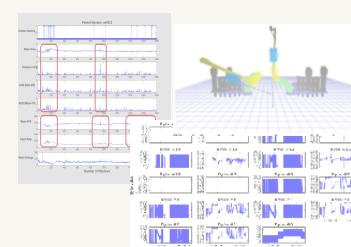
- Hazard analysis to identify causes for **unsafe scenarios**
- Software fault-injection to **create realistic hazards**



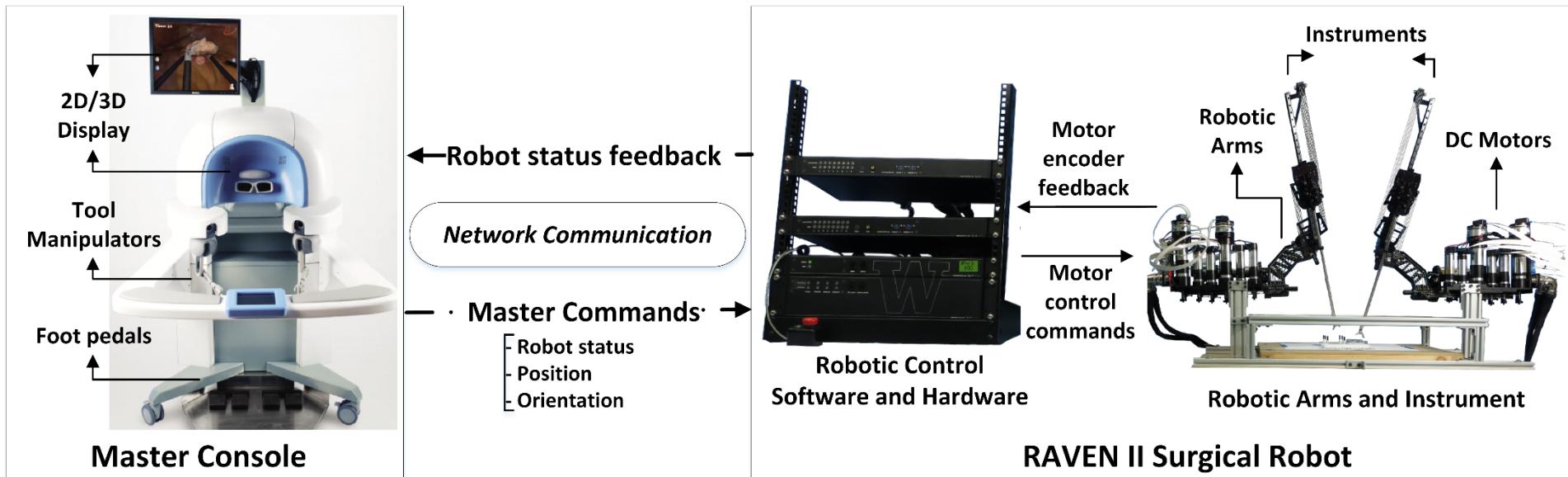
## Resilient Medical Cyber-Physical Systems

### Designing Resilient Systems

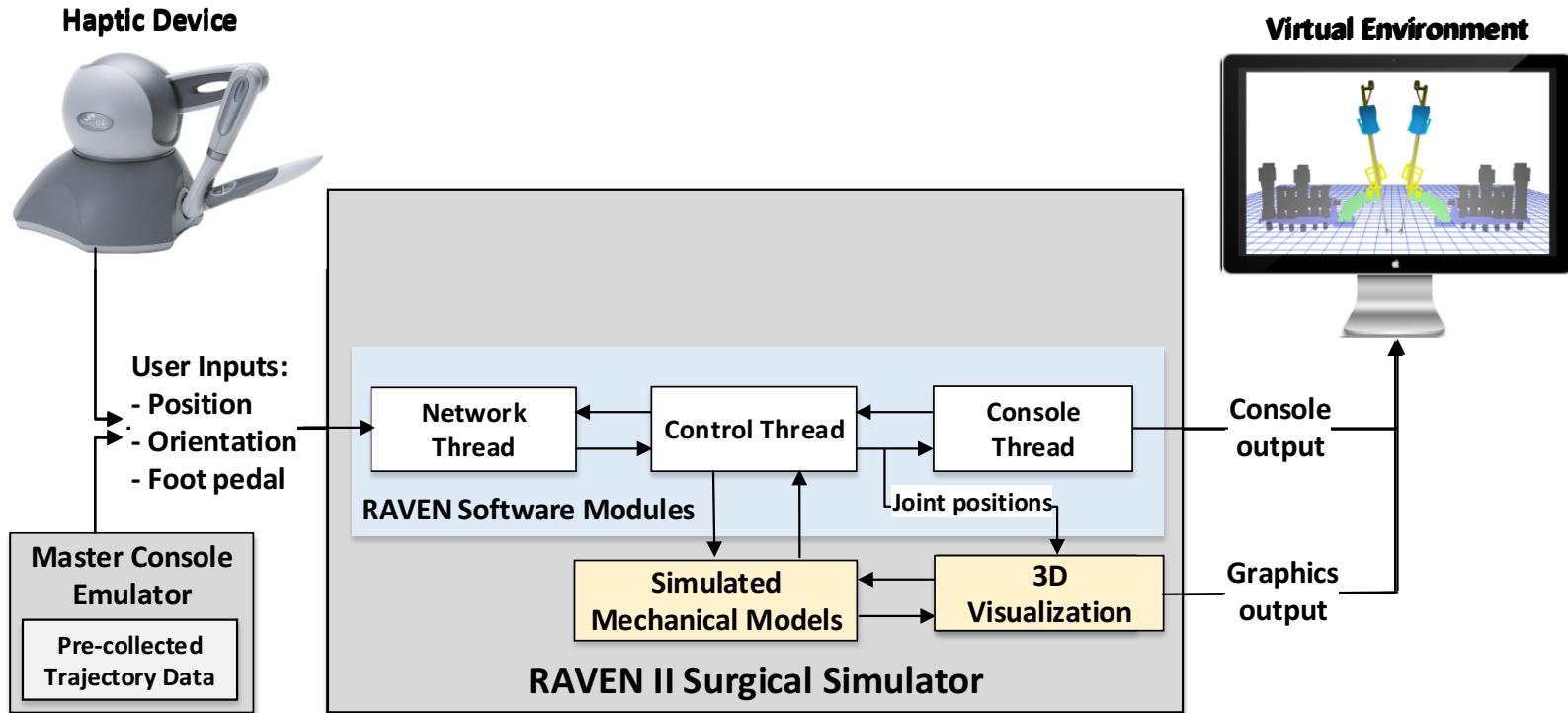
- Real-time detection and mitigation of safety hazards
- Safety validation in presence of accidental failures or malicious attacks



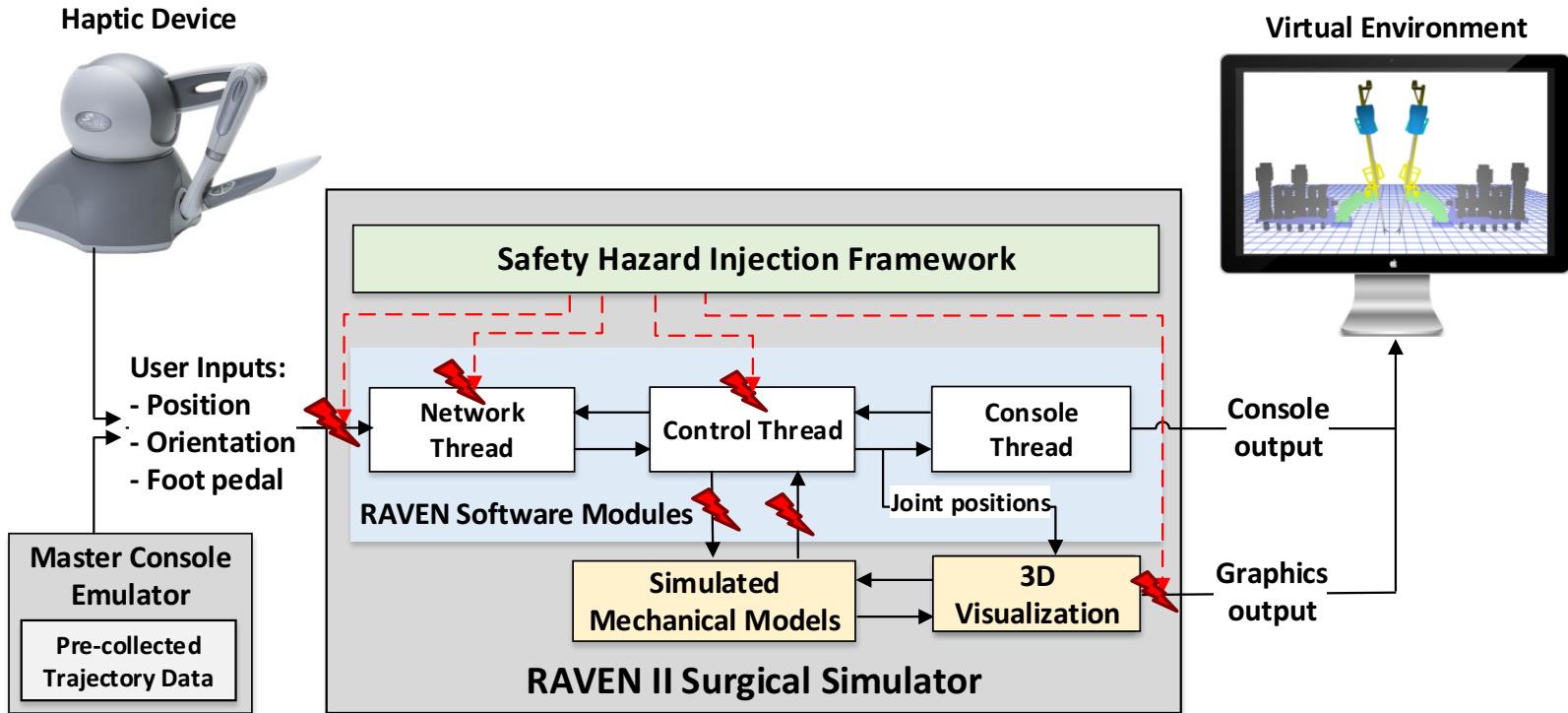
# Safety Hazard Simulation



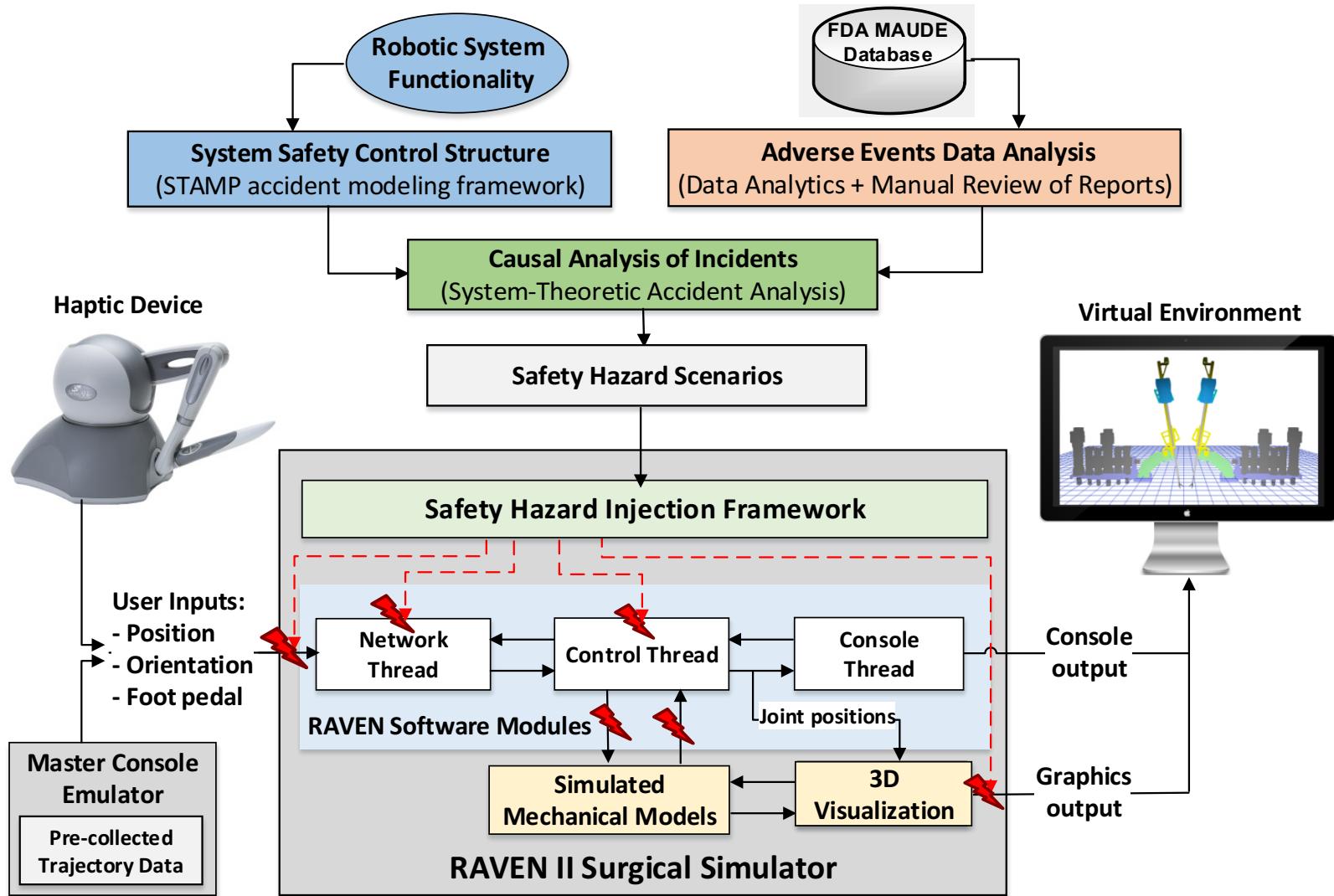
# Safety Hazard Simulation



# Safety Hazard Simulation

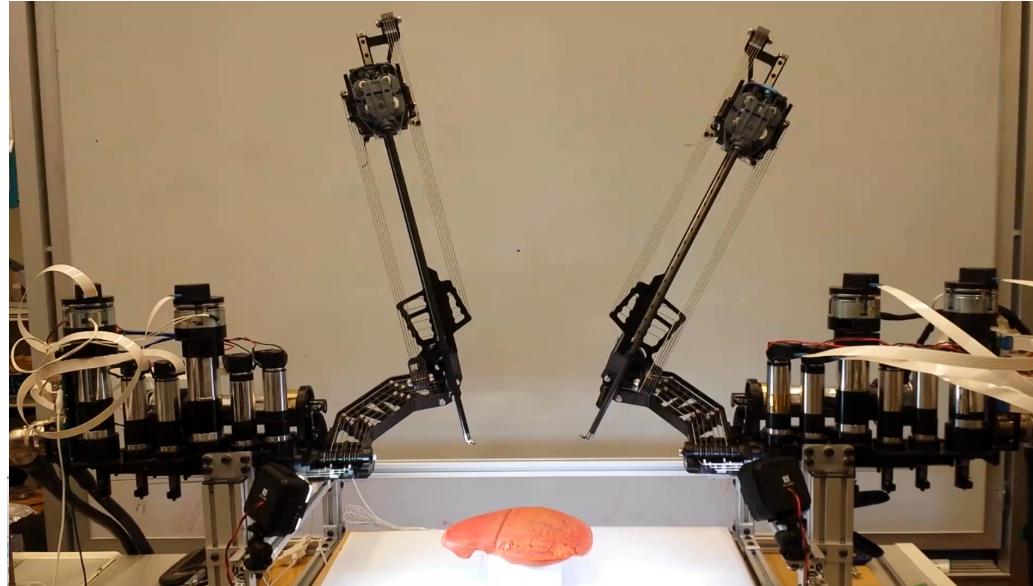


# Safety Hazard Simulation

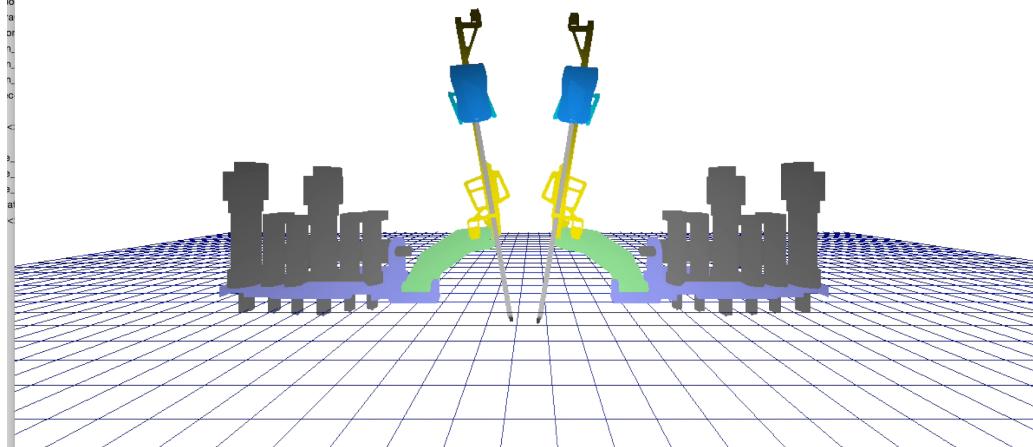


# Safety Hazard Simulation

Safety  
Validation

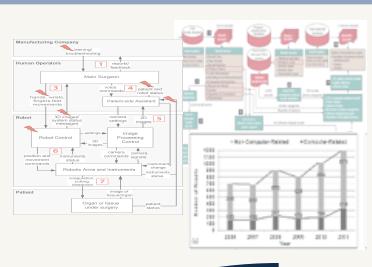


Safety  
Training



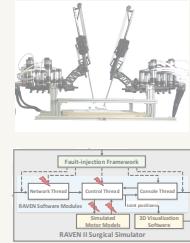
## Analyzing Data on Past Safety Incidents

- Large-scale analysis of incident reports
- Systems-theoretic causality modeling



## Assessing Resilience to Safety Hazards

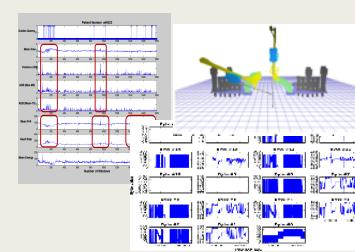
- Hazard analysis to identify causes for unsafe scenarios
- Software fault-injection to create realistic hazards



## Resilient Medical Cyber-Physical Systems

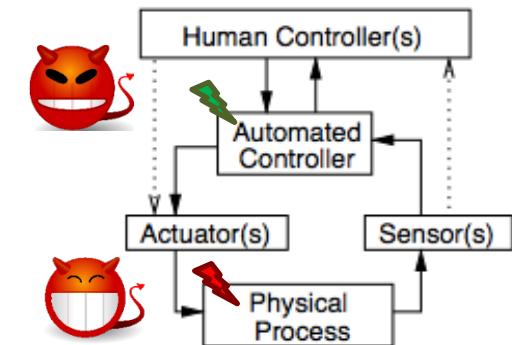
### Designing Resilient Systems

- Real-time detection and mitigation of safety hazards
- Safety validation in presence of accidental failures or malicious attacks



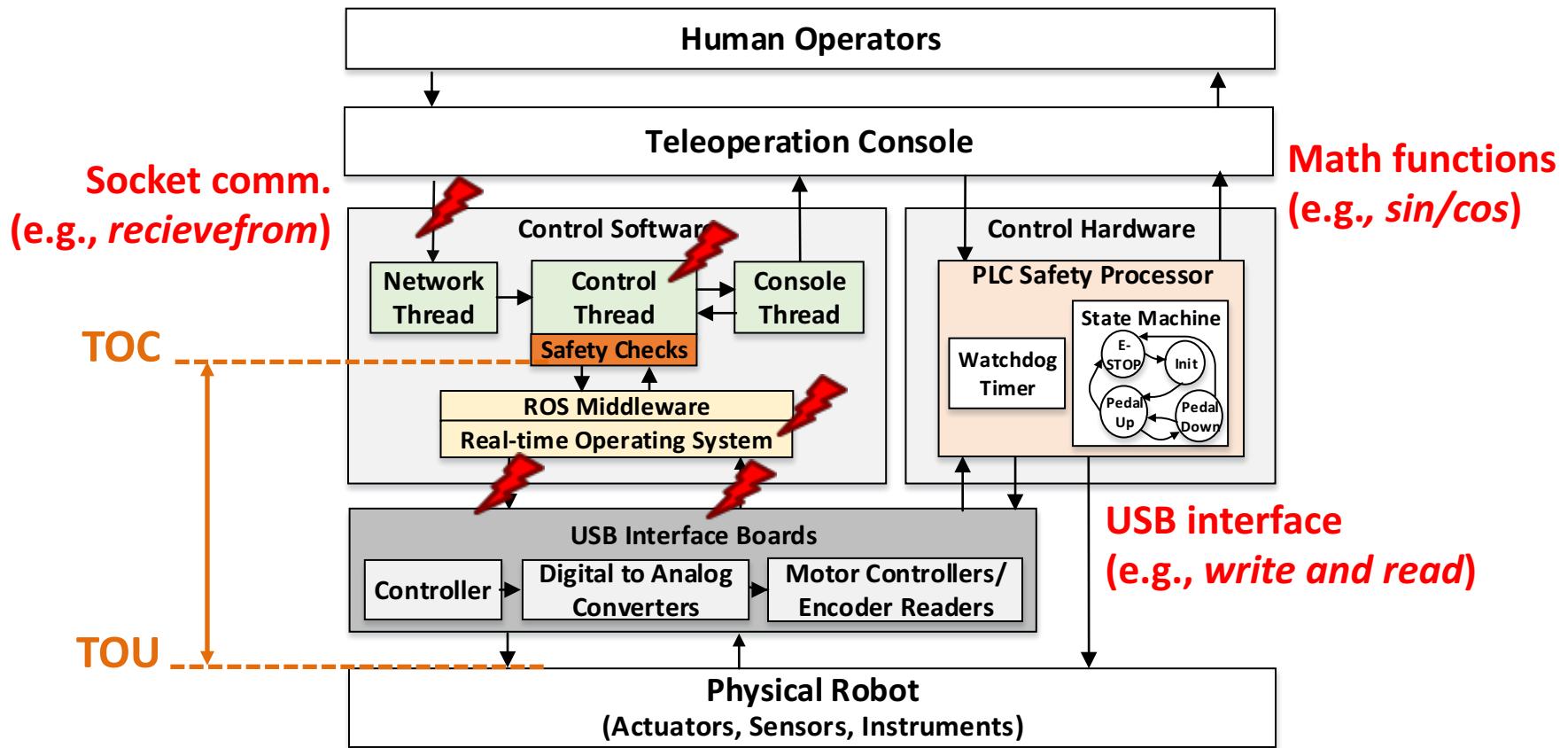
# Safety-Critical Cyber-Physical Attacks

- **Initiated in cyber domain, launched in physical layer**
  - Installs a self-triggered malware
  - Exploits vulnerabilities in OS or control software
  - Analyzes system activity to infer a *critical time*
  - Injects maliciously-crafted commands
- **Directly result in violation of safety constraints and catastrophic impact in physical domain:**
  - Damage the physical system or harm the patient
- **Hard to distinguish from accidental failures and human errors**

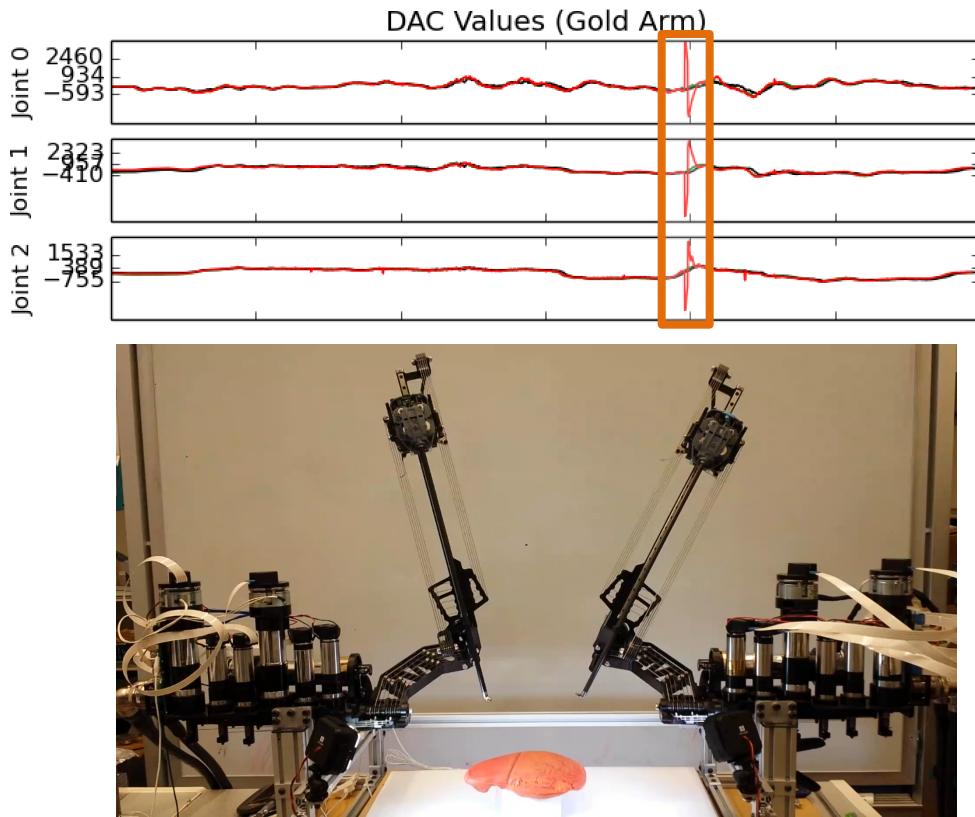


# Vulnerabilities in Control System

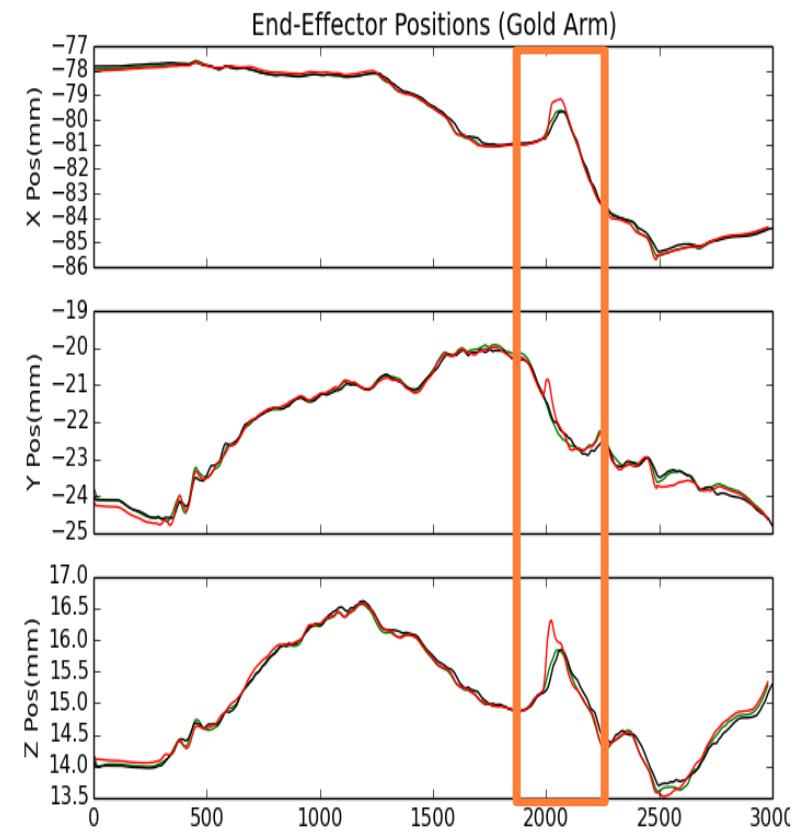
- Time of Check To Time of Use (TOCTTOU) gap
- Dynamic loading of system libraries



# Simulated Safety Hazards

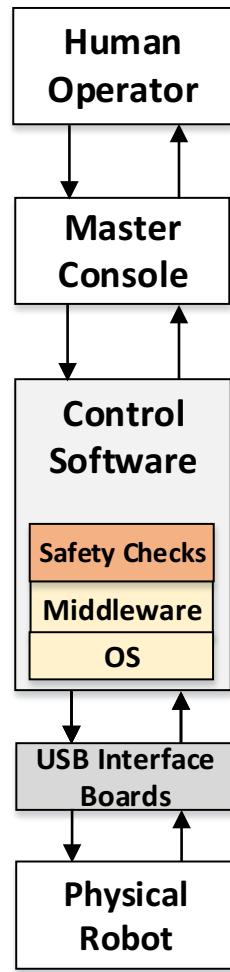


Inject error to control commands issued from control software to robot



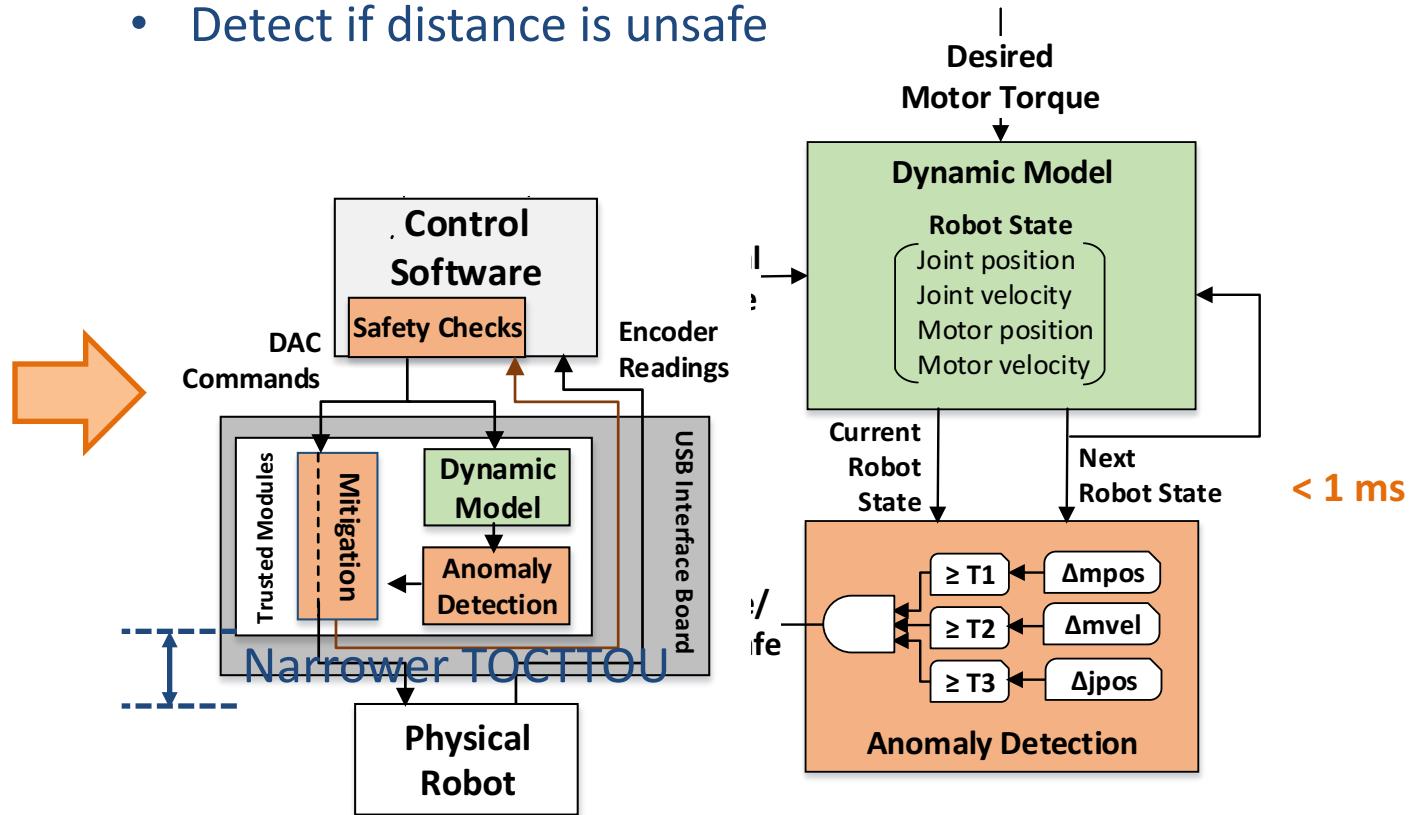
Abrupt jump of end-effector  
> 1mm change in arm position in one control cycle

# Dynamic Model Based Detection



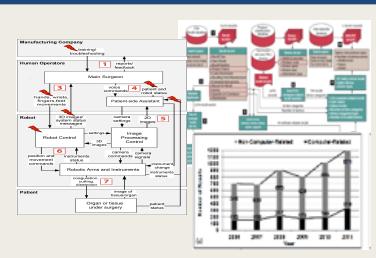
## Preemptive detection of safety hazards

- Real-time computation of joint/motor dynamics
- Estimation of next robot state
- Detect if distance is unsafe



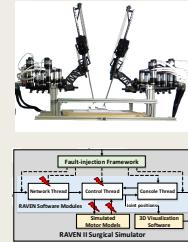
## Analyzing Data on Past Safety Incidents

- Automated analysis of incident reports
- Systems-theoretic causality modeling



## Assessing Resilience to Safety Hazards

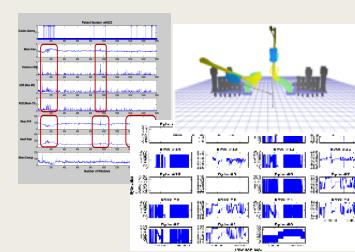
- Hazard analysis to identify causes for **unsafe scenarios**
- Software fault-injection to **create realistic hazards**



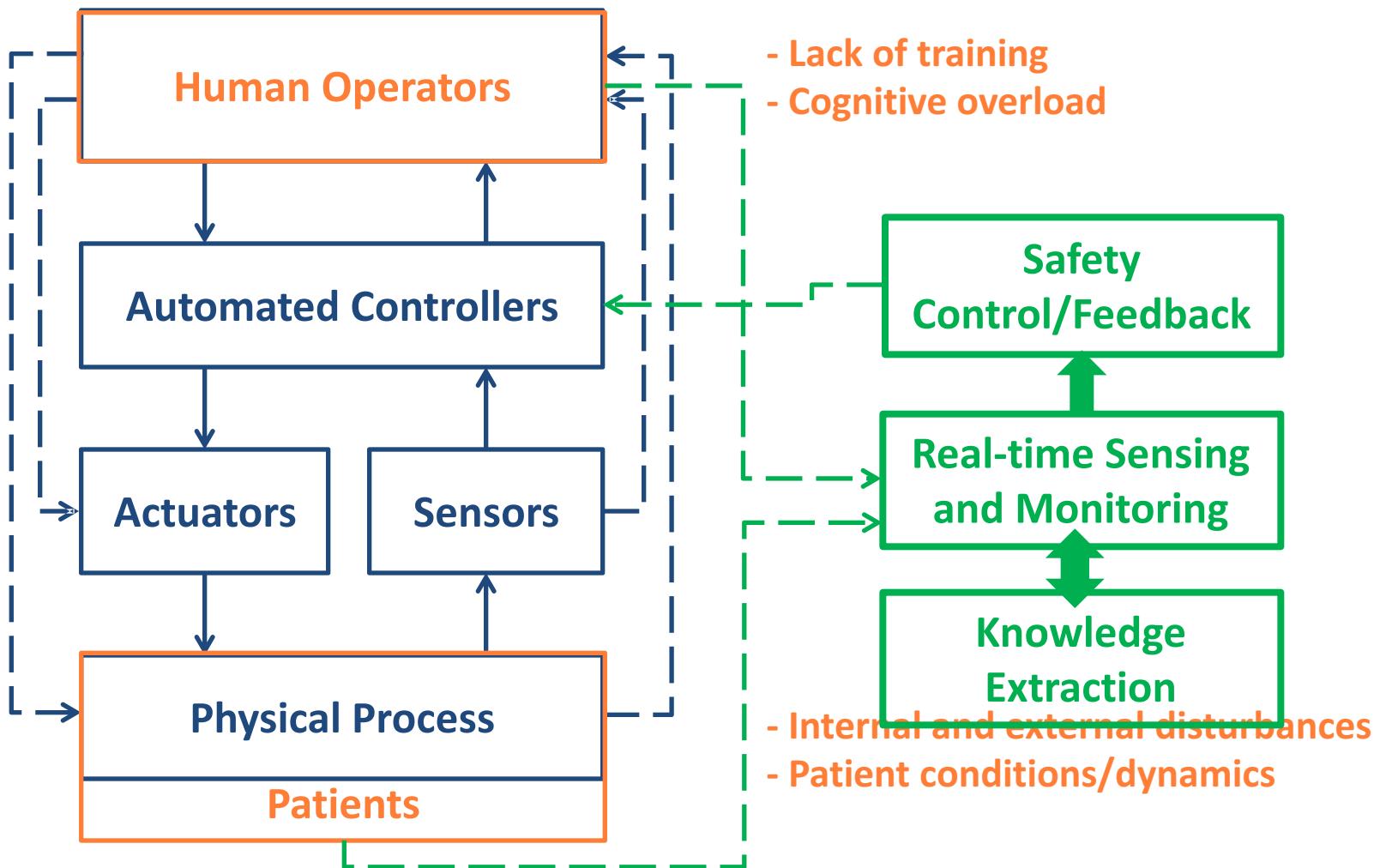
## Resilient Medical Cyber-Physical Systems

### Designing Resilient Systems

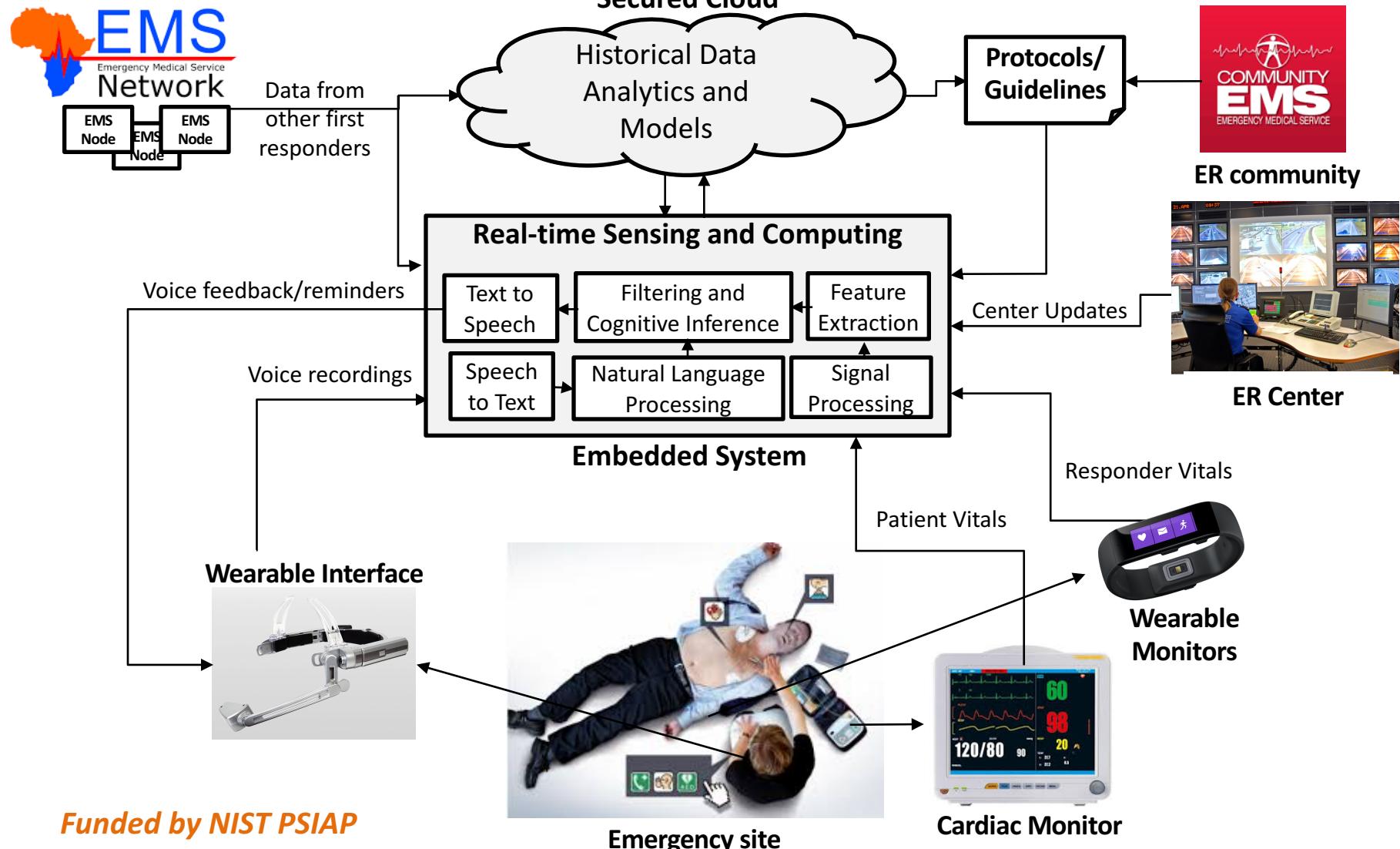
- Real-time detection and mitigation of safety hazards
- Safety validation in presence of accidental failures or malicious attacks



# Context-Aware Safety Engines



# Cognitive Assistant Systems for EMS



# Publications

## Analysis of Medical Device Recalls and Adverse Event Reports:

### 1. “Automated Classification of Computer-based Medical Device Recalls,”

H. Alemzadeh, R. Hoagland, Z. Kalbarczyk, R. K. Iyer,

In the *27th IEEE International Symposium on Computer-Based Medical Systems (CBMS'14)*.

### 2. “Safety Implications of Cardiothoracic Robotic Surgery:

**Analysis of Adverse Event Reports of da Vinci Surgical Systems,”**

H. Alemzadeh, J. Raman, N. Leveson, R. K. Iyer,

Presented as J. Maxwell Chamberlain Memorial Paper for the Adult Cardiac Surgery in the *50th Annual Meeting of the Society of Thoracic Surgeons (STS'14)*, Jan. 2014.

**Featured in Wall Street Journal, “Report Raises Concerns on Robotic Surgery Device”, Nov. 8, 2013.**

### 3. “Safety Implications of Robotic Surgery: A Study of 14 Years FDA Data on da Vinci Surgical Systems,”

H. Alemzadeh, J. Raman, N. Leveson, Z. Kalbarczyk, R. K. Iyer,

CSL Technical Report, UILU-ENG-13-2208, Nov. 2013, *PLoS ONE*, vol. 11, no. 4: e0151470, 2016

**Featured in the MIT Technology Review, BBC, NBC News, Daily Mail, Gizmodo, and others, July 2015.**

### 4. “Analysis of Safety-Critical Computer Failures in Medical Devices,”

H. Alemzadeh, R. K. Iyer, Z. Kalbarczyk, J. Raman,

*IEEE Security & Privacy (IEEE S&P'13)*, vol. 11, no. 4, pp. 14-26, July-Aug. 2013.

## Safety and Security of Teleoperated Surgical Systems:

5. “A Hardware-in-the-loop Simulator for Safety Training in Robotic Surgery”  
**X. Li, H. Alemzadeh, D. Chen, Z. Kalbarczyk, R. K. Iyer, T. Kesavadas**  
*In the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2016.*
6. “Targeted Attacks on the Control Systems of Teleoperated Surgical Robots”  
**H. Alemzadeh, D. Chen, X. Li, T. Kesavadas, Z. T. Kalbarczyk, R. K. Iyer**  
*In the 46th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016*
7. “Safety-critical Cyber-Physical Attacks: Analysis, Detection, and Mitigation”  
**H. Lin, H. Alemzadeh, D. Chen, Z. Kalbarczyk, R. K. Iyer**  
*In the Symposium and Bootcamp on the Science of Security (HOTSON), 2016.*
8. “Systems-theoretic Safety Assessment of Telerobotic Surgical Systems”  
**H. Alemzadeh, D. Chen, A. Lewis, Z. Kalbarczyk, J. Raman, N. Leveson, R. K. Iyer**  
*In the 34th International Conference on Computer Safety, Reliability, and Security (SAFECOMP), Delft, Netherlands, September 2015.*
9. “A Software Framework for Simulation of Safety Hazards in Robotic Surgical Systems”  
**H. Alemzadeh, D. Chen, Z. Kalbarczyk, R. K. Iyer, X. Li, T. Kesavadas, J. Raman**  
*In the 6th Medical Cyber Physical Systems Workshop, Hosted at CPS Week, Seattle, WA, April 2015.*
10. “Simulation-based Training for Safety Incidents: Lessons from Analysis of Adverse Events in Robotic Surgical Systems” [Poster]  
**H. Alemzadeh, Z. Kalbarczyk, R. K. Iyer, T. Kesavadas, S. Small, J. Raman,**  
*In the American College of Surgeons' 8th Annual Meeting of the Consortium of ACS-accredited Education Institutes, March 2015.*