Resilience of Medical Devices and Systems

Ravishankar K. Iyer

In collaboration with:
Homa Alemzadeh, Daniel Chen, Zbigniew Kalbarczyk
Electrical and Computer Engineering, UIUC

Jai Raman MD PhD
Cardiac Surgery, Rush University Medical Center
Real-time Continuous Monitoring: To save lives and reduce healthcare cost

- Adaptive – from hospital to home
- Individual- and disease-specific monitoring

Early Prediction of Patient Deterioration: To prevent life-threatening events (e.g. in ICUs)

- Multimodal signal analysis and fusion
- Machine learning techniques

Fusion:
Medical records, Physiological signals, Genome data

Integration of Safety, Reliability, Security: To ensure accurate and robust processing

- From specification to design to deployment
- Safety-driven design

Validation, Testing, and Benchmarking: To uncover safety and reliability holes

- Application specific error detectors
- Stochastic modeling, model checking, fault injection
- From specification to design to deployment

Designing Safe, Reliable, and Secure Medical Devices

- Formal analysis models and tools
- Include the human operators in the loop

Designing:
Custom Hardware, Light-weight sensors

Stochastic modeling, model checking, fault injection

Safety analysis tools

- Include the human operators in the loop

- From specification to design to deployment
- Safety-driven design

Application specific error detectors
Examples: Catastrophic Medical Device/System Failures

GE Healthcare - Telemetry Monitoring Systems.
Did not alarm a series of ventricular fibrillation events.
**Patient Outcome:** Death

FDA Adverse Event Report - 2010

Boston Scientific - Thermal endometrial ablation system
Defective circuit board could result in loss of system pump
**Potential Patient Impact:** Hot fluid 90°C into uterus.

FDA Recall - 2009

Medtronic - Defibrillator/Monitor
Short circuit in the PCB, Result, not delivering energy
**Potential Patient Outcome:** Death

FDA Recall - 2007
Examples: Security and Privacy Vulnerabilities

**Fuji Film Medical System – Computed Radiography Workstation**
A computer virus infecting six systems caused images get frozen on the screen and not being transferred to radiography reader.

*Patient Outcome:* Delay in treatment.

*FDA Adverse Event Report - 2010*

**Boston Scientific – iLab Ultrasound Imaging System**
Infected by a computer malware (worm) that could infect the computer network connected to it.

*Potential Patient Impact:* FDA Recall - 2008

**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*
Computer Failures in Medical Devices

- 17K recall records between 2007 and 2013:
  - 6,864 (40%) unique failure events
  - 1,678 (24%) computer-based medical devices
  - More than 200 (12%) safety-critical:
    - Physical safety hazards, patient injuries, and death
  - Increasing number of computer-related recalls: doubled since 2007

- Software was the major cause (64.3%)
- But Hardware and Battery (20.8%) failures were 2.8 times more costly
- Impacted 6.5 million (54.4%) of devices on market

Defibrillators
17 Recalls – 415K devices
293 Deaths, 14K Injuries
-Delayed/failed shock delivery
-Premature shutdown

Implantable Pacemakers
1 Recall – 40K devices
60 Deaths, 3,201 Injuries
-Loss of rate response
-Premature battery depletion

Infusion Pumps
15 Recalls – 945K devices
23 Deaths, 574 Injuries
-Loss of rate response
-Premature battery depletion

Physiological Patient Monitors
10 Recalls – 38K devices
4 Deaths, 79 Injuries
-Delayed audible alarms
-Failure to restart

Surgical Robots
19 recalls => 109,709 devices on the market
10,624 adverse events (2000-2013)
144 deaths, 1,391 injuries, 3,933 malfunctions
-System crash/Lockup during the surgery
-Power loss during the surgery
-Manipulation and control failure
Example: Robotic Surgical Systems

- 3-D magnified view of surgical field through surgeon’s
- Small incisions to allow the scope/robotic arms into the body
- 7 degrees of freedom in instruments to mimic hand/wrist movements
Adverse Events in Robotic Surgery

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

- An increase in reporting of adverse events, 32 times since 2006
- Rates of adverse events per procedure is relatively constant.

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%)

88.3% of all reports

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

Examples from the FDA Databases

<table>
<thead>
<tr>
<th>Report No. (Year)</th>
<th>Summary Description</th>
<th>Inadequate Operational Practices</th>
<th>Procedure Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>921167 (2007)</td>
<td>Patient-side manipulator dropped suddenly. Scissors instrument bumped into uterus.</td>
<td>Surgeon removed his/her hands from master manipulators before removing his/her head from console viewer (keeping head in the console viewer keeps the robot engaged)</td>
<td>Pierced patient’s uterus</td>
</tr>
<tr>
<td>1961862 (2010)</td>
<td>Endoscopic camera manipulator difficult to move. Master tool manipulator drifted when released. Instrument moved to guided tool change mode, moved slightly forward, and bumped into colon.</td>
<td></td>
<td>Punctured patient’s uterus</td>
</tr>
<tr>
<td>2644122 (2012)</td>
<td>Uncontrolled movement of master manipulators.</td>
<td></td>
<td>Injury to patient’s colon</td>
</tr>
<tr>
<td>2636117 (2012)</td>
<td>Limited range of motion and drift while master tool manipulators were used, even after system restart.</td>
<td></td>
<td>Damaged abdominal wall</td>
</tr>
<tr>
<td>2422359</td>
<td></td>
<td></td>
<td>Aborted after 1.75 hours</td>
</tr>
</tbody>
</table>
**MedSafe:**
Analysis of Failures and Safety Incidents

http://web.engr.illinois.edu/~alemzad1/MedSafe/
Aviation Accident Rates:
All: 0.23 to 0.51
Fatal: 0.01 to 0.07

Rate of Robotic Surgery Injury or Death Events (Robotic Surgery Accidents per 100,000 procedures)
Confidence Interval 95% - Trends calculated for 2006-2012

Aviation Accident Statistics by NTSB (1992-2011)
(Accident per 100,000 flight departures)
From: http://www.ntsb.gov/data/aviation_stats.html

Robotic Surgery Accident Rates:
All: 188 to 845
Safety-Critical: 32 - 50

Constant Rates of Fatalities, 1-2 order of magnitudes

Aviation Accident Rates:
All: 0.23 to 0.51
Fatal: 0.01 to 0.07
Accidents and Hazards in Robotic Surgery

Accidents:
- ACC1: Patient expires during or after the surgery.
- ACC2: Patient or surgery staff are injured during the surgery.
- ACC3: Patient experiences serious complications after the surgery.
- ACC4: Robotic system or an instrument is damaged.

Injectable Security Hazards:

<table>
<thead>
<tr>
<th>Hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
</tr>
<tr>
<td>H2</td>
</tr>
<tr>
<td>H3</td>
</tr>
</tbody>
</table>
Safety Challenges

• Accidents/vulnerabilities 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
Experimental Assessment 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 emulators that prepare surgical trainees on how to deal with safety incidents

• Augment the surgical robots/emulators with fault-injection capabilities

• Simulate realistic safety hazard scenarios extracted from data

• In collaboration with:
  • RUSH University and University of Chicago Medical Centers

Systems-theoretic Analysis of Accident Causes

- Causes are not limited to “component failures” or “human errors”.
- Accidents are complex processes resulted from:
  - Violation of safety-constraints at different layers of the system
  - Spanning from physical system to human operators, to manufacturers and regulators
  - Unintentional flaws or intentional malicious actions in the system

- Robotic surgical system produced a system error code during a procedure.
  - The error reoccurred even after resetting the system.
  - Surgeon decided to continue using a manual camera manipulation for 5-6 hours
  - A loss of carbon dioxide insufflation occurred resulting in heart pushing up into the endoscope, causing lacerations to patient’s right ventricle.
  - Total procedure time = 14 hours!

  - Fault Origin: Faulty electronics (printed circuit assembly, remote arm controller)
  - Error Symptom: System Error indicating communication failure between modules
  - Patient Outcome: Life Threatening Injury

FDA MAUDE Database – MDR Report 2240665
Example: A cyber-physical Compromise of a Robotic Tele-Surgical Systems

Fault Model:
- Unexpected USB disconnection
- Motor controller malfunctions

Threat Model:
- Adversary has unauthorized root access to the host system controlling the robot

Attack:
- Corrupts USB packets sent to the motor controllers altering control current
USB Corruption Malware

1. Loads a malicious wrapper on Linux shared libraries
2. Installs the injector as a kernel module
3. Analyzes the system calls to find target file descriptors
4. Analyzes the running processes to find the robot thread ID
5. Runs a USB sniffer to find the best time to start the attack
6. Calls malicious library functions to send bad USB packets at critical right time to robot
7. Robot USB board receives a bad command and the robot jumps!!
Impact: Sudden Jump of Robotic Arms
Fault/attack-injection Testbed & Framework

- Emulates realistic safety/security hazard scenarios (informed by the FDA data)
- Automated 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
- 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 the results and visualization in virtual 3D environment
  - Hardware: An Arduino Uno microcontroller added for automatic start and stop of RAVEN PLC System
System-theoretic Emulation of Safety Hazards

Robotic System Functionality

System Safety Control Structure (STAMP Accident Modeling technique)

Causal Analysis of Incidents (System-Theoretic Accident Analysis)

Safety Hazard Scenario Library

Adverse Event Data Analysis (Data Analytics: Text mining/machine learning)

Hazard Injection Strategies

Safety Hazard Injection Engine

Robotic Surgical Simulator

Robotic Software Modules

Master Control Inputs

Graphics Output

User Interface

Graphic Processing

Robotic Control
Experiments on RAVEN II Robot: Injection of Realistic Hazard Scenarios

<table>
<thead>
<tr>
<th>Safety Hazard Scenario</th>
<th>Fault Type or Malicious Action</th>
<th>Target Software Module</th>
<th>Target Variables</th>
<th>No. Manifested/Injected Faults</th>
</tr>
</thead>
</table>
| 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  
Improper human operation or patient-side manipulator malfunction | Control Thread  
*(get_USB_packet)*  
Control Thread  
*(put_USB_packet)* | USB Board address or returned status  
USB Board address or returned status | 61/64  
10/12 |
| Unintended Instrument Movements (sudden jumps) | Corruption of USB packets sent to hardware by getting unauthorized access to the OS or RAVEN software | Control Thread  
*(put_USB_packet)* | DAC commands sent to robotic joints | 3/4* |
Non-recoverable System Error Simulated on RAVEN II Robot
STAMP: Systems-theoretic causality modeling and analysis of accidents [Leveson, 2011]

System’s Safety Control Structure:

Unexpected failures or intentional malicious actions leading to unsafe control
Robotic System Safety Control Structure

Control Action Generation
- Decide on the placement of ports, arms, and instruments
- Decide on the surgical trajectories and motions
- Interpret and troubleshoot the system problems
- Decide to continue or interrupt the procedure

Process Model
- Procedure status: Time, intraoperative status
- Robotic system status: System errors
- Arms and instruments status

Console Controls:
- Master controls, foot pedals, pod controls
- Hand/foot movements

Main Surgeon
- Emerg. stop
- Clutch instr.
- Focus camera
- BI cautery
- Mono cautery
- Grip tissue
- Move instr.

Control Algorithm
- Translate the console commands to robotic motions
- Mathematical calculations to smooth out movements
- Monitor the status of arms and instruments
- Generate system status messages and errors
- Transfer the system to safety states

Robot Control
- Process Model
  - Arms and instruments status:
  - Engaged / dis-engaged
  - Insulated / Not insulated
  - Position and velocity
  - Vision status

Actuators:
- Electric motors, pneumatic actuators
- Arm and instrument commands

Robot Control
- 3D images from image processing control

Robot Arm and Instruments
- EndoWrist Instruments, Endoscopic Camera
- Coagulation, cutting, dissection
- Image of tissue/organ

Sensors:
- Encoders, potentiometers, health circuits
- Camera signals to image processing
- Status lights/signals to the assistants
# Example Safety Hazard Scenarios

<table>
<thead>
<tr>
<th>Type</th>
<th>Control Action</th>
<th>Context (System Condition)</th>
<th>UCA  No.</th>
<th>Possible Hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required Action Not Performed</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clutch instrument or emergency stop</td>
<td>Intraoperative urgency (bleeding, burning or damage to tissue)</td>
<td>UCA-1</td>
<td>H1 H3</td>
</tr>
<tr>
<td></td>
<td>Focus, move, or change settings of camera</td>
<td>Vision is lost, obstructed, out of focus, the endoscope not aligned with the target anatomy, or insufflation device has low CO₂ level</td>
<td>UCA-2</td>
<td>H1-4 H3</td>
</tr>
<tr>
<td></td>
<td>Disable instrument arm</td>
<td>Intraoperative urgency (bleeding, burning or damage to tissue), or arm/instrument malfunction</td>
<td>UCA-3</td>
<td>H1 H2 H3</td>
</tr>
<tr>
<td><strong>Hazardous Action Performed</strong></td>
<td>Cauterize or grip tissue</td>
<td>Intraoperative urgency (bleeding, burning or damage to tissue)</td>
<td>UCA-4</td>
<td>H1-2 H1-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Incorrect electro-cautery settings or instrument insulation broken</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Insufflation device has low CO₂ level or vision lost/obstructed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Power lost or system in error</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Instrument too close to another instrument or non-target anatomy</td>
<td></td>
<td>H1-4</td>
</tr>
<tr>
<td><strong>Incorrect Timing/Order</strong></td>
<td>Remove hands from manipulators</td>
<td>Before removing head from console viewer</td>
<td>UCA-5</td>
<td>H1-4 H3</td>
</tr>
<tr>
<td></td>
<td>Move camera arm</td>
<td>After camera arm is disabled</td>
<td>UCA-6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cauterize or grip tissue</td>
<td>Before the target instrument is activated (clutch instrument)</td>
<td>UCA-7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Before the target anatomy is gripped</td>
<td>UCA-8</td>
<td></td>
</tr>
<tr>
<td><strong>Incorrect Duration</strong></td>
<td>Cauterize tissue</td>
<td>Applied too long</td>
<td>UCA-9</td>
<td>H1-1 H1-3</td>
</tr>
<tr>
<td></td>
<td>Clutch instrument</td>
<td>Applied too short</td>
<td>UCA-10</td>
<td>H1-4 H3</td>
</tr>
</tbody>
</table>
STPA (Lev 2011): System-theoretic Hazard Analysis for both Safety and Security

Inexperienced Surgeon
- emerg. stop
- clutch instr.
- focus camera
- BI cautery
-Mono cautery
- grip tissue
- move instr.

Console control malfunctions or malicious corruption of user commands
- Console Controls: Master controls, foot pedals, pod controls

Software errors or malware
- Control Algorithm
  - Translate the console commands to robotic motions
  - Mathematical calculations to smooth out movements
  - Monitor the status of arms and instruments
  - Generate system status messages and errors
  - Transfer the system to safety states

Display failures or malicious disruption of console feedback
- 3D images from image processing control
- 3D images/ system status & messages
- Console Display: High-resolution stereoviewer, left and right eyes

Actuator failures
- Actuators: Electric motors, pneumatic actuators

Encoder failures
- Encoder failures
- 3D images/ system status & messages

Grasper failure
- Grasper failure
- 3D images/ system status & messages

Robot Control
- Process Model
  - Arms and instruments status:
  - Engaged / dis-engaged
  - Engaged / Not insulated
  - Position and velocity
  - Vision status

Robot Control
- Actuators: Electric motors, pneumatic actuators
- Actuator failures
- Encoder failures

Robotic Arms and Instruments
- EndoWrist Instruments, Endoscopic Camera
- coagulation, cutting, dissection
- image of tissue/organ
- camera signals to image processing
- status lights/signals to the assistants
- control actions by main surgeon
- control actions by the assistants
- position
- insert
- extract
- position
- exchange
- docking
- draping

Main Surgeon
- Process Model
  - Procedure status:
    - Time, Intraoperative status
  - Robotic system status:
    - System errors
    - Arms and instruments status

30
Inexperienced Surgeon
Console control malfunctions or malicious corruption of user commands
Software errors or malware
Display failures or malicious disruption of console feedback
RAVEN II Robotic Tele-surgical System

Master Console

- 2D/3D Display
- Tool Manipulators
- Foot pedals

RAVEN II Surgical Robot

- Robot status feedback
- Network Communication

Master Commands

- Robot status
- Position
- Orientation

Robotic Control Software and Hardware

- Motor encoder feedback
- Motor control commands

Instruments
- DC Motors

Robotic Arms

Robot status feedback

Master Commands

Network Communication

Emergency stop/restart

User commands

Robot status feedback

Software Modules

- Network Thread
- Control Thread
- Console Thread

Hardware Modules

- PLC Safety Processor
- USB Interface Board
- Motor Controllers

Raven II Control System
Running a Pre-collected Trajectory on RAVEN II Robot