Seventh Annual Cyber-Physical Systems Principal Investigators' Meeting

Arlington, VA | October 31 – November 1, 2016

Project Title: 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**

University of Illinois at Urbana-Champaign

Challenges

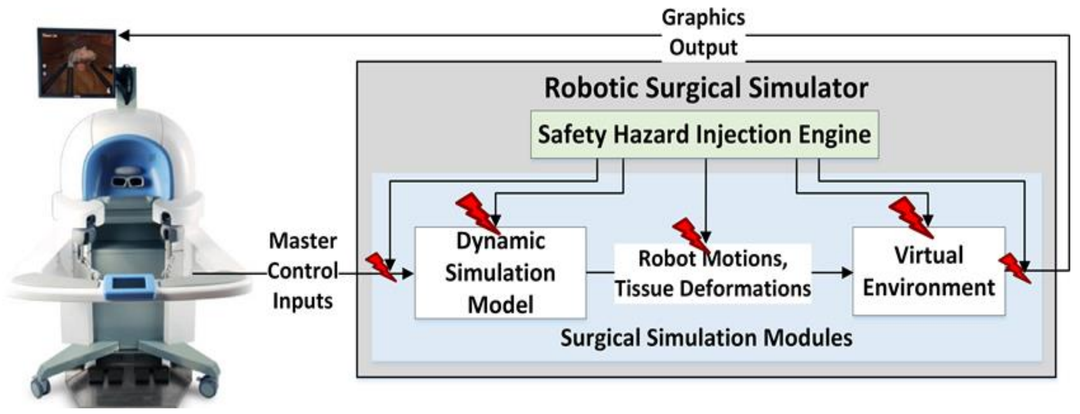
- Timely and accurate detection, prediction, and mitigation of incidents during surgery.
- An in-depth analysis of incident causes, which takes into account the complex interactions among the system components, human operators, and patients and identifies multi-dimensional causes leading to incidents.
- Safety, reliability, and resiliency assessment of the robotic systems in the presence of realistic safety hazards, reliability failures, and malicious tampering with the system.
- Continuous monitoring for detection of safety, reliability, and security violations to enable timely recovery or migration in a safe state.

Technical Approach

- Develop a framework that integrates:
- A ***systems engineering approach*** to identify causal factors that lead to hazards that cause accidents in the context of the target surgical robot
- A ***robotic surgical simulator*** (based on the control software of the RAVEN II robot) to allow modeling the behavior of human operators, the dynamics of robotic hardware and mechanical components, and tool-tissue dynamics.
- A ***safety hazard injection engine*** integrated with the surgical simulator and the actual robot to perform hazard injection and assess resiliency of the proposed monitoring environment.
- A ***safety monitoring engine***, which combines knowledge of prior accidents with continuous real-time system monitoring to detect hazards and enable timely mitigation/recovery actions.

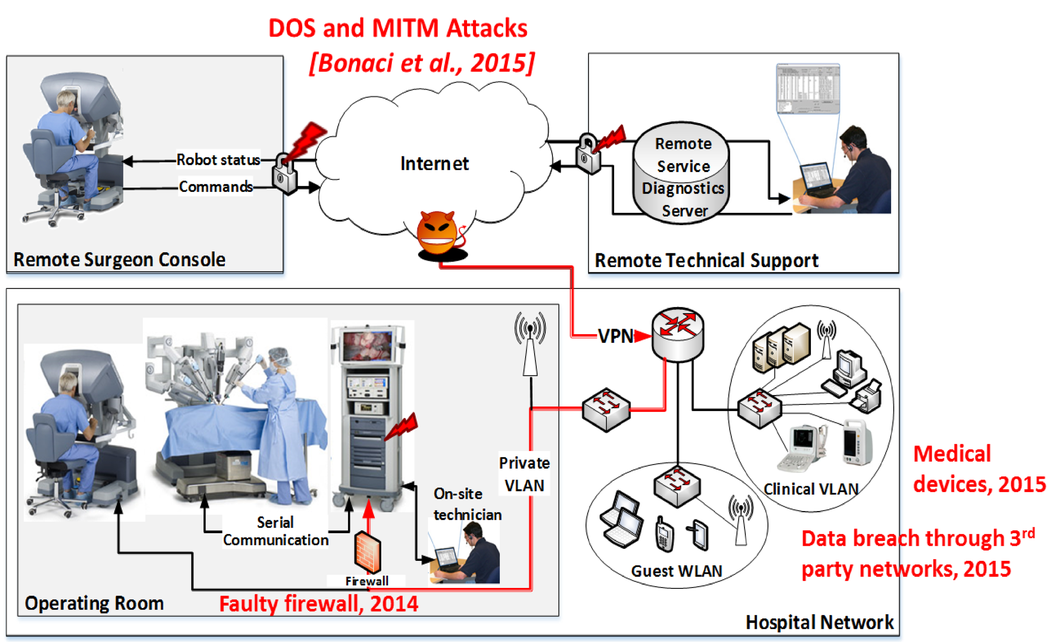
CNS 1545069;
University of Illinois at Urbana-Champaign
Contacts: R. K Iyer (rkiyer@illinois.edu);
Z. Kalbarczyk (kalbarcz@Illinois.edu),
and T. Kesavadas (kesh@Illinois.edu)

Simulation of Safety-Related Scenarios



Hazard Scenario	Example System-related Causal Factors	Method to Recreate Hazards	Mutated Simulator Software Module/Function/Input
H1. Master controller malfunctions	Foot pedal doesn't work, pinch doesn't register	Surgeon inputs get corrupted before being transferred to the robot control	Faulty input stream
H2. Slave robot/device malfunctions	Robotic instrument jumps uncontrollably to an unintended location	Slave controller translates the surgeon's commands into incorrect motor and actuator signals	Faulty dynamic simulation model Faulty motion mapping)
H3. Console display malfunctions	Camera cable breaks, vision is foggy	Image is lost or obstructed	Faulty graphics (rendering failure) or faulty output stream (image stuck-at blank)
H4. Instrument malfunctions	Grasper not closed, instrument not recognized by the system,	Instrument stuck at closed or open	Faulty dynamic simulation model (instrument status stuck)
H5. System errors	System freezes: unrecoverable system errors	System doesn't respond to input and displays an error or blank image	Faulty dynamic simulation model (physics engine or motion mapping failure)

Simulation of Cyber-Physical Attack Scenarios



Scientific Impact

- CPSs face the threat of malicious attacks that exploit vulnerabilities in the cyber domain as footholds to introduce safety violations in the physical processes.
- 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).

Broder Impact

- Strategy for design and assessment of a broad class of control cyber-physical systems, which involve human in the on-line decision making loop.
- Broadening participation in multi-disciplinary projects spanning medicine and engineering.
- Introducing topics on resilient cyber-physical systems into graduate courses and undergraduate laboratories.
- Collaboration with academic institutions and industry partners to demonstrate the application of proposed analytics, validation techniques, and tools.
- 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.

References

1. H. Alemzadeh, D. Chen, Z. Kalbarczyk, R. K. Iyer "Targeted Attacks on Teleoperated Surgical Robots: Dynamic Model-based Detection and Mitigation," Int'l Conference on Dependable Systems and Networks, DSN 2016.
2. H. Alemzadeh, et al., "Safety Implications of Robotic Surgery: A Study of 13 Years of FDA Data on da Vinci Surgical Systems," 50th Annual Meeting of the Society of Thoracic Surgeons (STS), 2014.
3. H. Alemzadeh, R. K. Iyer, Z. Kalbarczyk, J. Raman, "Analysis of Safety-Critical Computer Failures in Medical Devices," IEEE Security and Privacy, vol. 11, no. 4, pp. 14-26, July/August 2013.