CAREER: Context-Aware Runtime Safety Assurance in Medical Human-Cyber-Physical Systems

Homa Alemzadeh, University of Virginia

https://www.nsf.gov/awardsearch/showAward?AWD_ID=2146295

Challenges

- Offline risk assessment and verification methods are inadequate in *preventing* adverse events.
- *Patient dynamics* and *human operator actions* complicate anomaly detection and runtime recovery.
- Solely data-driven and model-driven methods suffer from scarcity of data and complexity of models.

Solution

- A hierarchical framework for workflow modeling and task segmentation in robotic surgery (IJCARS'23, RA-L'23)
- Real-time multimodal context inference and activity recognition (ICRA'23, IROS'23, ICRA'24)
- Context-specific safety assurance cases and runtime monitors for ML-enabled MCPS, such as artificial pancreas systems (TDSC'23, SafeAI'23)

Scientific Impact

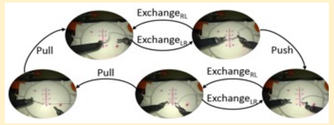
- Bridge the gap between offline formal modeling and runtime monitoring to enable resilient *human-in-the-loop* CPS.
- Develop an *integrated model and data-driven approach* for design of *safety engines* that combine domain knowledge, human-cyber-physical context, and operator/patient profiles for hazard *prediction* and *mitigation*.
- Design principles for safety engines applicable to medical, robotics, and autonomous systems.

Thrust 1
Safety Context Specification and Learning

Formal Framework for Control-Theoretic Hazard Analysis

$$G_{[t_0,t_e]}((\text{BG}>\text{BGT}\wedge\ \text{BG'}>0)\wedge(\text{IOB'}<0\wedge\ \text{IOB}<\beta_1)\Rightarrow\neg\ u_1)$$
$$G_{[t_0,t_e]}((\text{BG}>\text{BGT}\wedge\ \text{BG'}>0)\wedge(\text{IOB'}=0\wedge\ \text{IOB}<\beta_2)\Rightarrow\neg\ u_1)$$
$$G_{[t_0,t_e]}((\text{BG}>\text{BGT}\wedge\ \text{BG'}<0)\wedge(\text{IOB'}>0\wedge\ \text{IOB}<\beta_3)\Rightarrow\neg\ u_1)$$
$$G_{[t_0,t_e]}((\text{BG}>\text{BGT}\wedge\ \text{BG'}<0)\wedge(\text{IOB'}<0\wedge\ \text{IOB}<\beta_4)\Rightarrow\neg\ u_1)$$
$$G_{[t_0,t_e]}((\text{BG}>\text{BGT}\wedge\ \text{BG'}<0)\wedge(\text{IOB'}=0\wedge\ \text{IOB}<\beta_5)\Rightarrow\neg\ u_1)$$

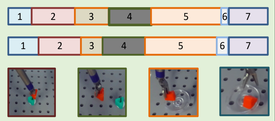
Modeling of Operational Context



Data-Driven Refinement of Context-Specific Safety Properties

Thrust 2
Runtime Human-Cyber-Physical Context Inference

Task Segmentation and Activity Recognition



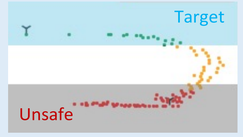
Cyber Control Policy and Physical State Estimation

Multi-modal Data

Dynamic Models

Thrust 3
Just-in-Time Risk-Aware Response and Mitigation

Human-Cyber-Physical Reachability Analysis



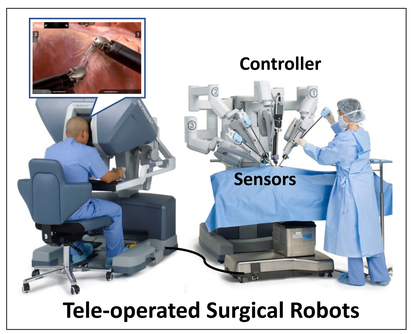
Hazard Likelihood Estimation

Response Action Generation

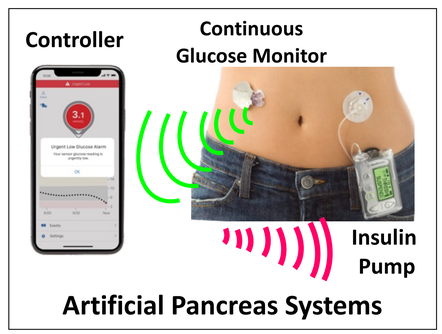
Context-Specific Action Selection

Broader Impact

- Improve *situational awareness* by timely and accurate hazard detection, potentially reducing number of adverse events and risk of harm to patients.
- Promote participation of *undergraduate researchers and K-12 students* from diverse backgrounds in the areas of engineering and robotics in medicine.



Tele-operated Surgical Robots



Artificial Pancreas Systems

Award ID#: **2146295**