Activity-Aware Error Recovery in Tele-Operated Surgical Robots

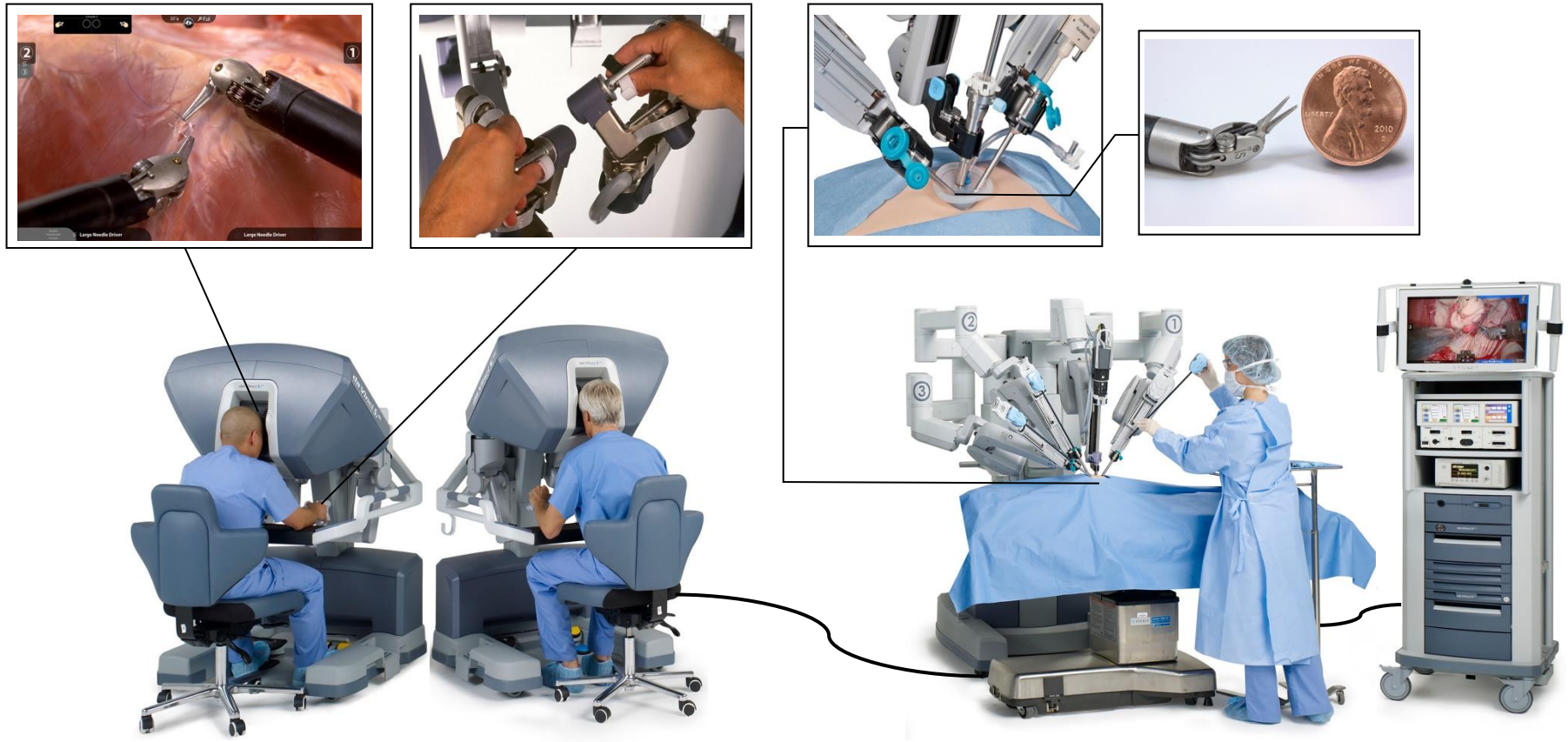
Homa Alemzadeh

Dependable Systems and Analytics (UVA-DSA)

Electrical and Computer Engineering

Computer Science (by courtesy)

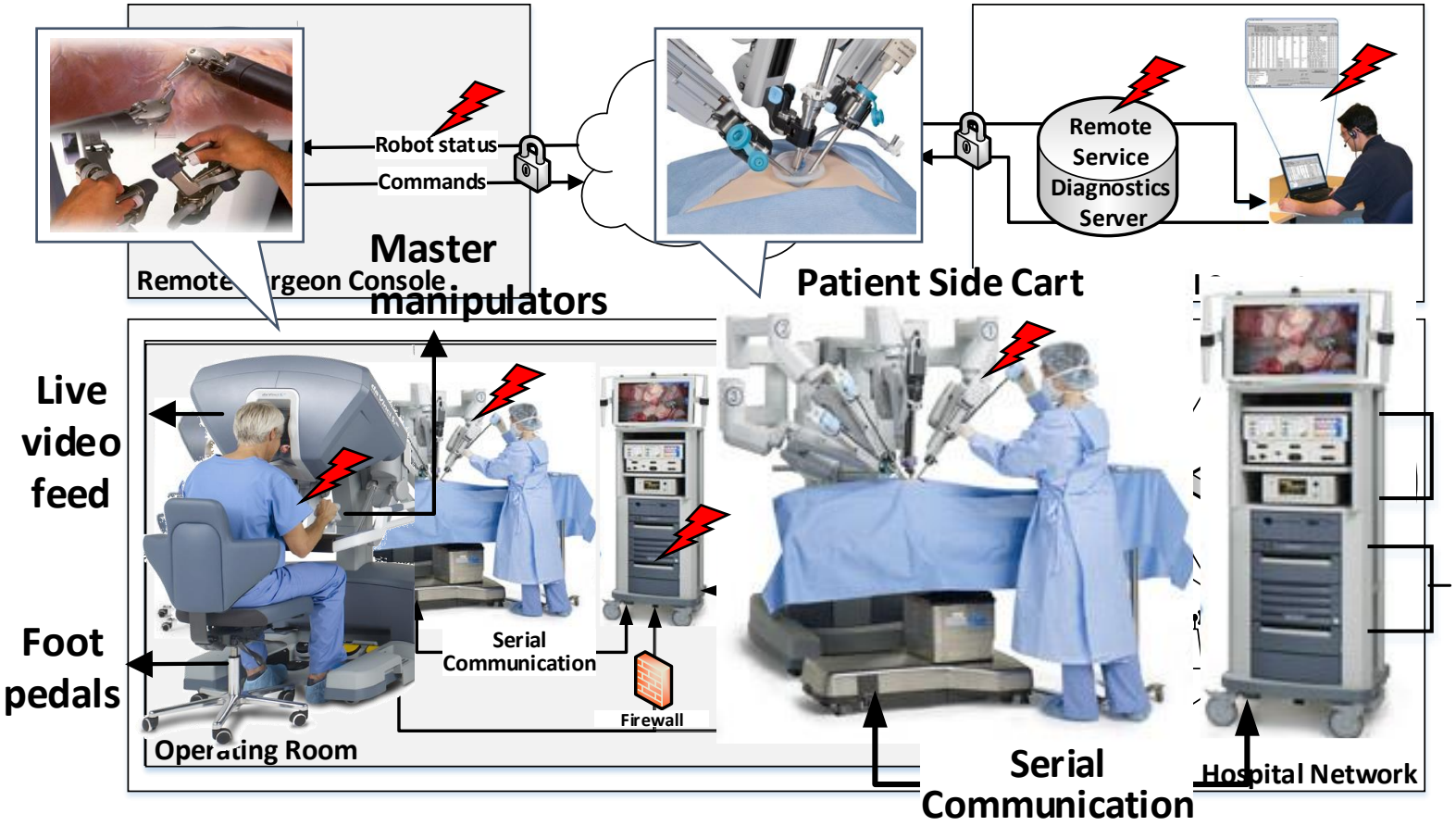
Tele-operated Surgical Robots



Loosely Closed-loop Semi-autonomous: No haptics, limited vision feedback

Credits: da Vinci Surgical System, Intuitive Surgical, Inc.

Human-Cyber-Physical Systems



Unintended Human Errors *[IJMRCAS 2022]*

Software, hardware, mechanical faults *[PLOS ONE 2016]*

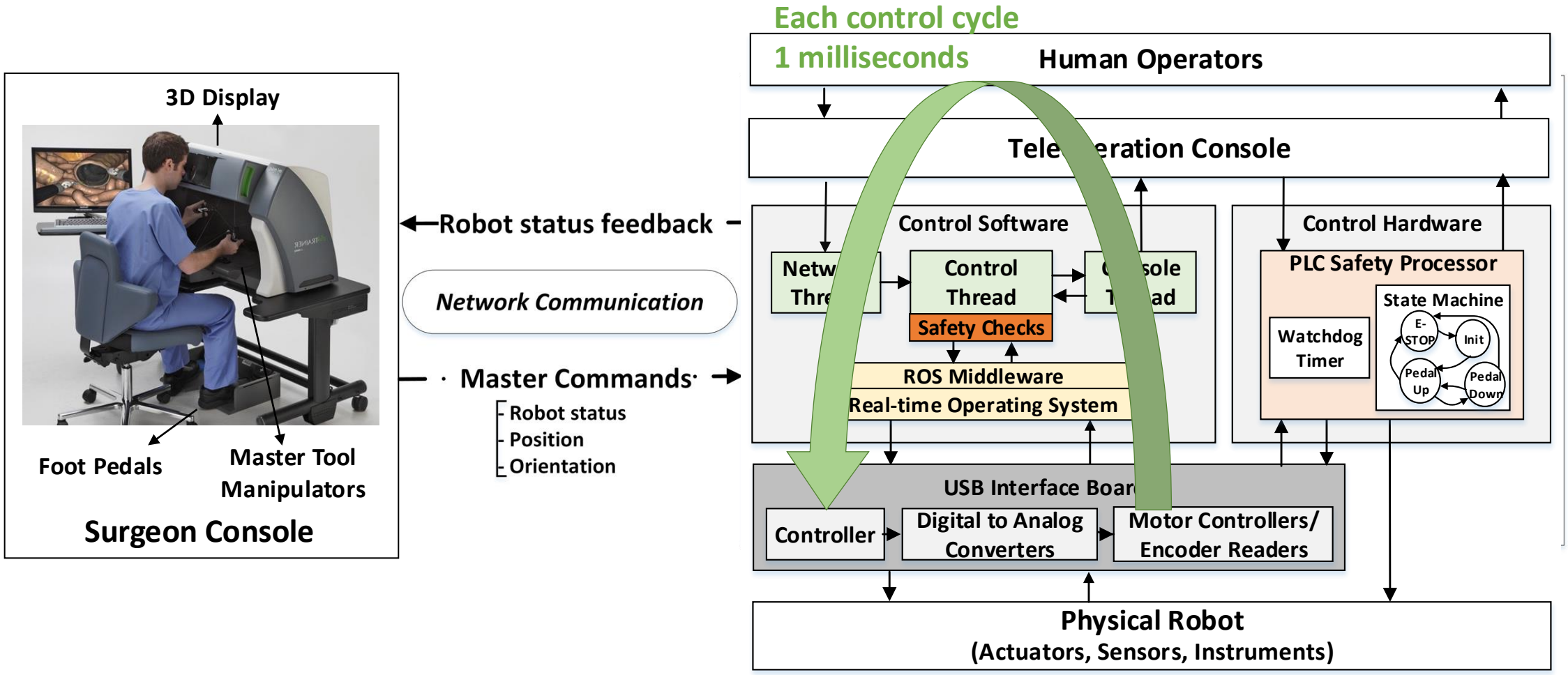
DOS and MITM Attacks *[ICCPS 2015]*

Faulty firewalls *[WIRED 2014]*

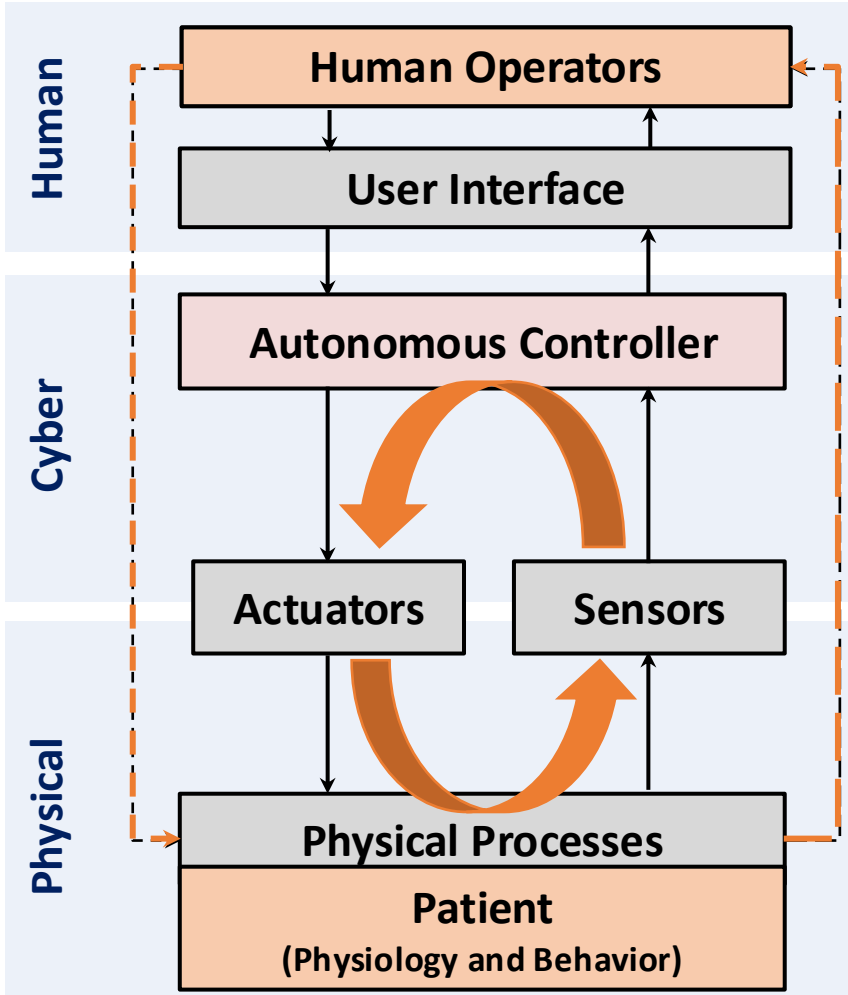
Malware targeting control software *[DSN 2016]*

H. Alemzadeh, *et al.,* "Adverse Events in Robotic Surgery: A Retrospective Study of 14 Years of FDA Data". *PLOS ONE*, 2016.
K. Hutchinson, *et al.,* "Analysis of Executional and Procedural Errors in Dry-lab Robotic Surgery Experiments," *IJMRCAS*, 2022.
H. Alemzadeh, *et al.*, "Targeted Attacks on Teleoperated Surgical Robots: Dynamic Model-Based Detection and Mitigation", *IEEE DSN*, 2016.

Tele-operated Surgical Robot Platform



Human-Cyber-Physical Systems

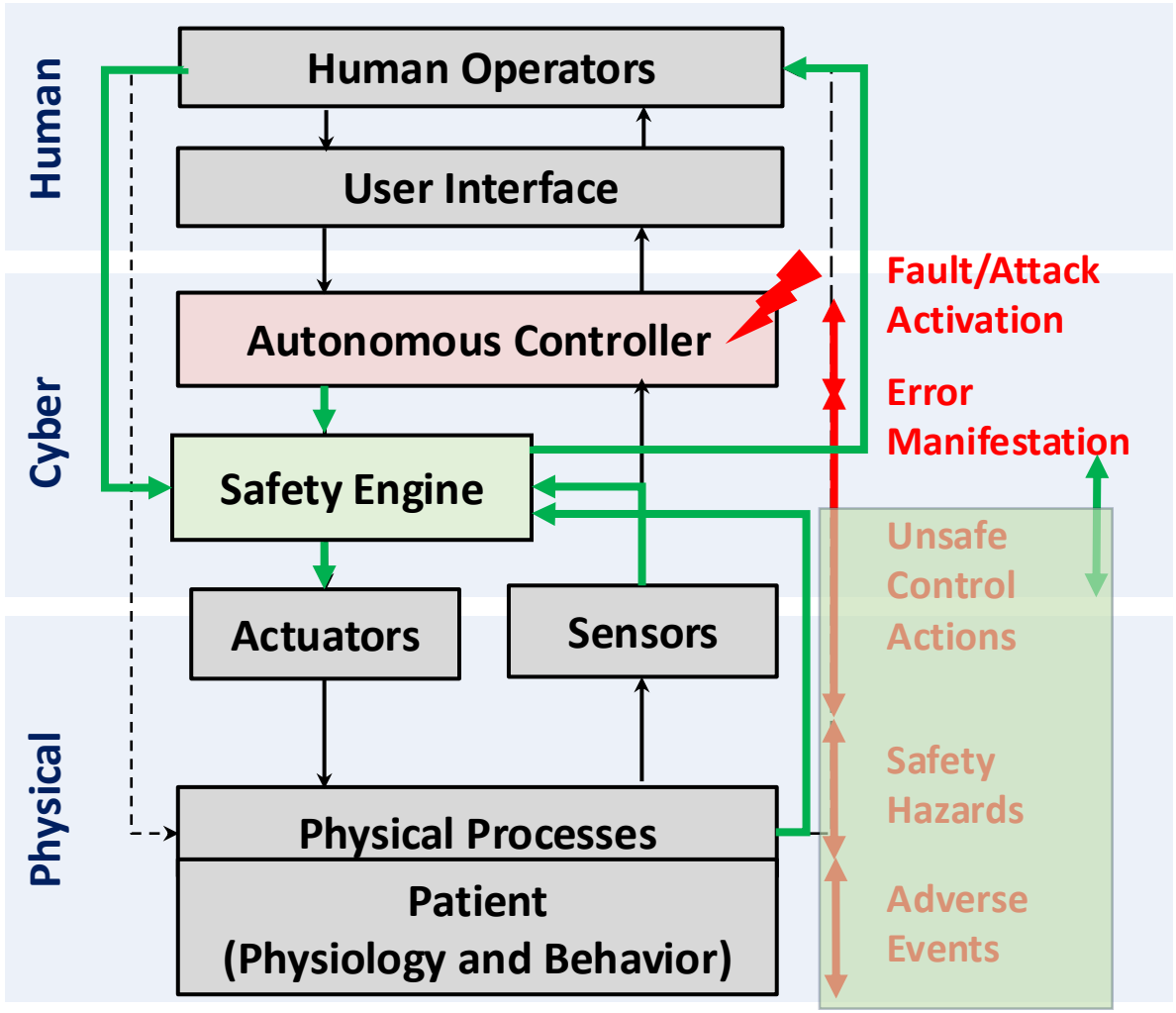


- Human supervision and control
- Tele-operation
- Advanced expertise and operational workflows

- Complex and interconnected software
- AI-enabled perception and control
- Tight timing and resource constraints

- Diverse and unexpected operational scenarios
- Variety of patient profiles & environmental factors
- Physiological and behavioral dynamics

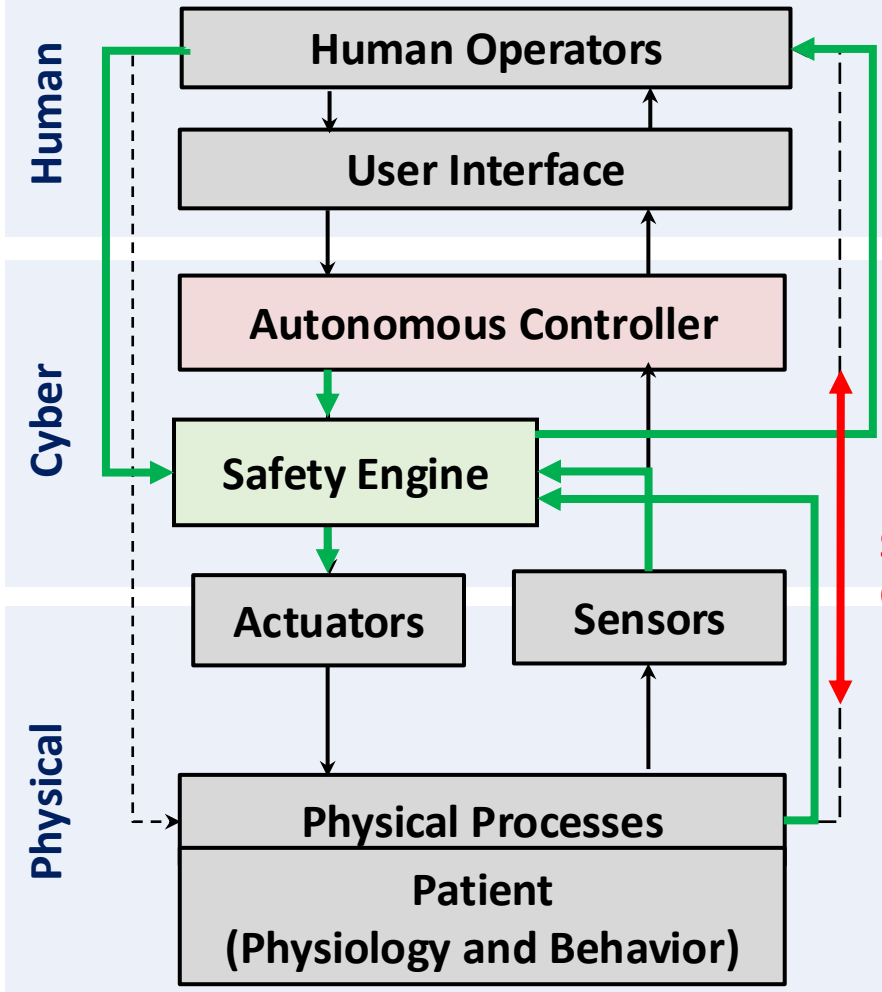
Runtime Safety Assurance



Runtime Safety Engines

- **Preemptive Detection of Unsafe Control Actions**
  - Based on sensor data and control commands
  - Just before execution in the physical layer
- **Prediction of Safety Hazards**
  - Hazard time and likelihood estimation
- **Prevention of Adverse Events**
  - **Automated** mitigation and recovery
  - **Feedback** to human operators

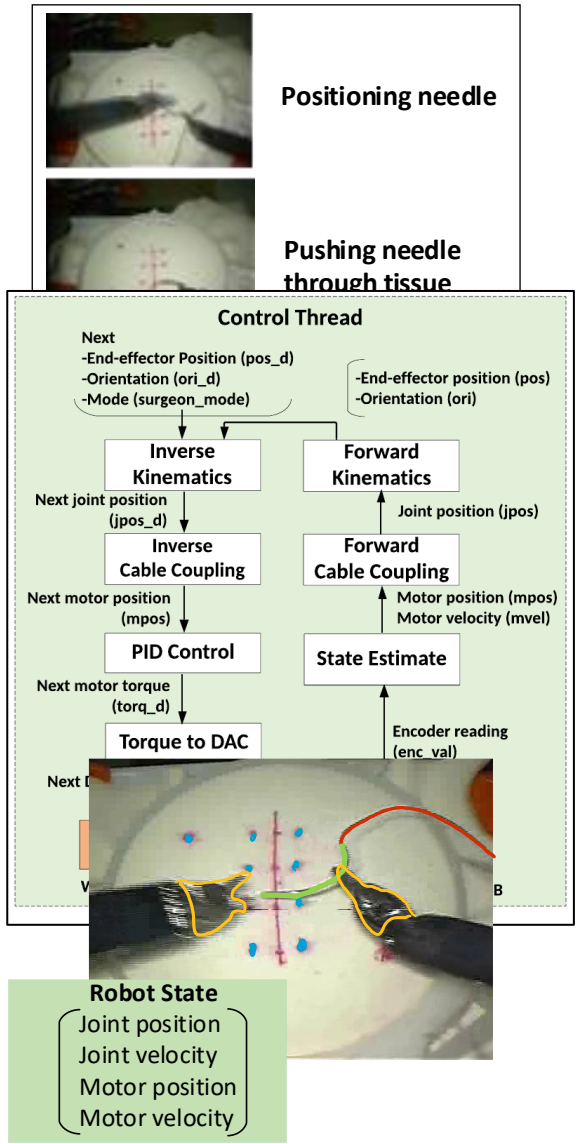
Context-Aware Safety



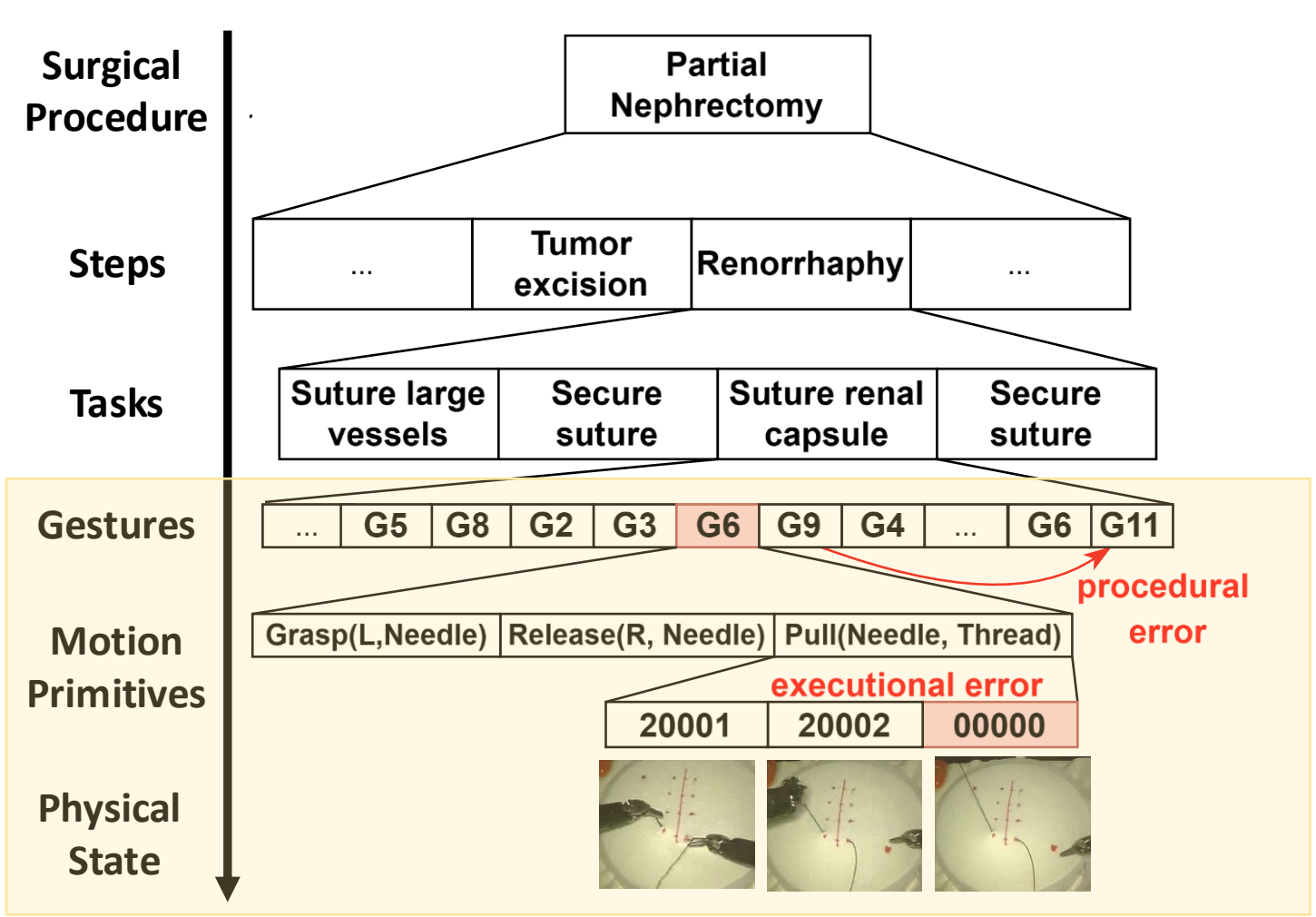
- **Operational Context**
  - Operator workflows, tasks, actions
  - User intent, style, and skill level
- **Cyber Context**
  - Control system and software states

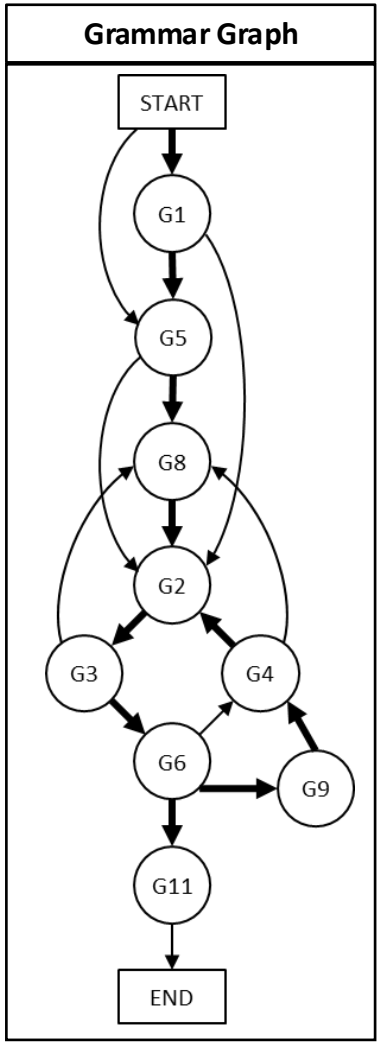
Safe or Unsafe Control Action?

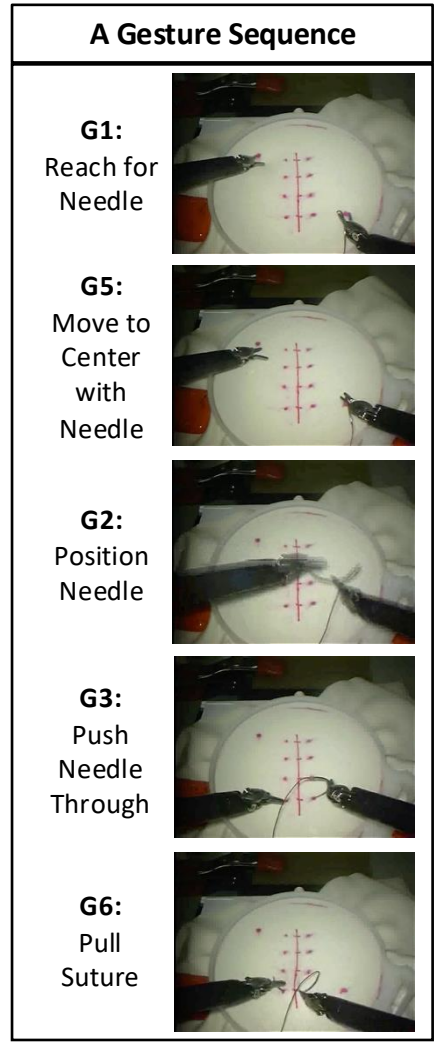
- **Physical Context**
  - Physical and environmental states
  - Patient profiles and dynamics



Operational Context in Surgery

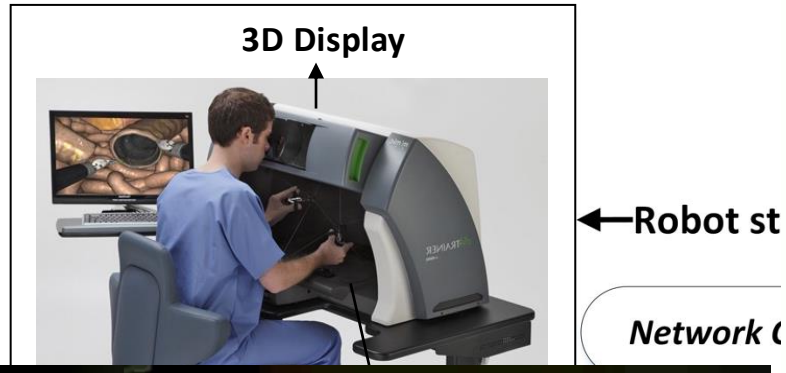


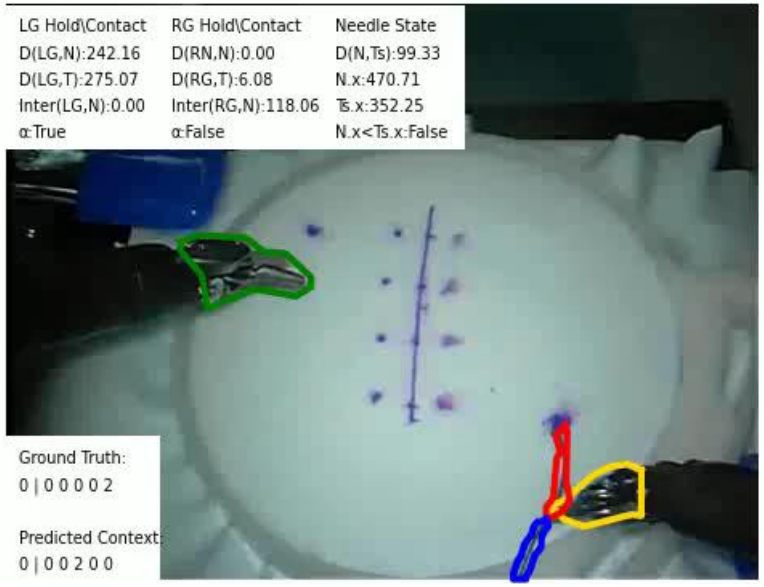


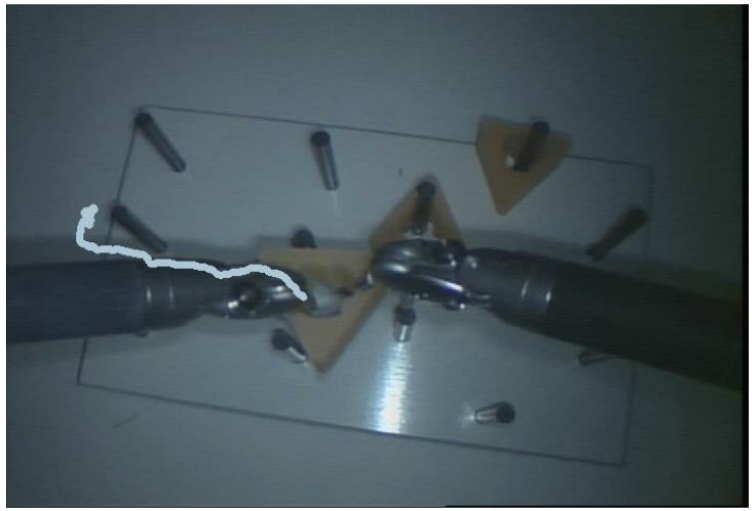


K. Hutchinson, I. Reyes, Z. Li, H. Alemzadeh, "COMPASS: A Formal Framework and Aggregate Dataset for Generalized Surgical Procedure Modeling," *IJCARS 2022.*

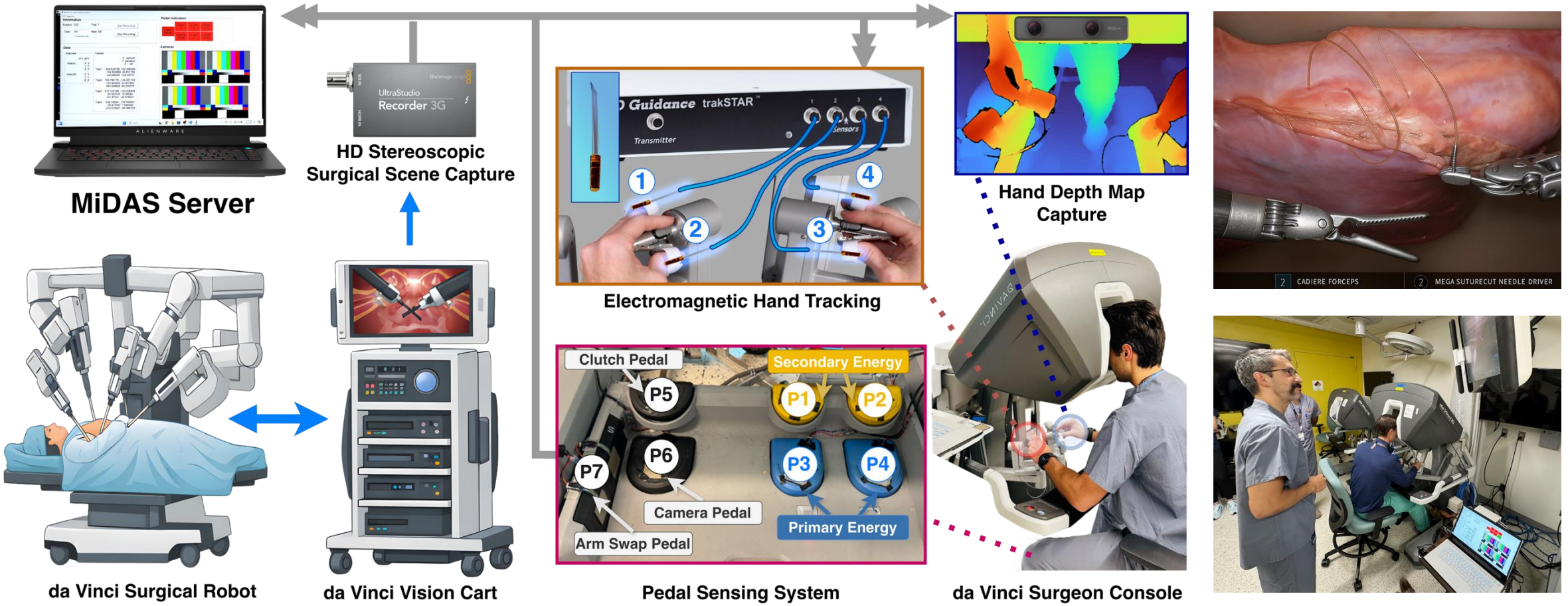
Context-Aware Safety Engine







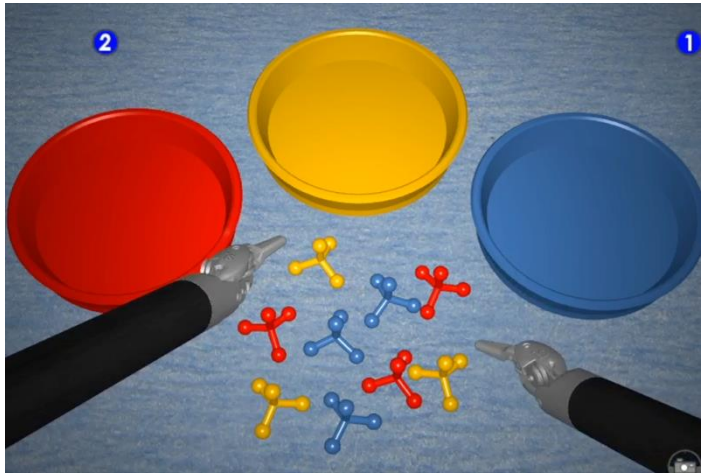
MiDAS: Multimodal Data Acquisition

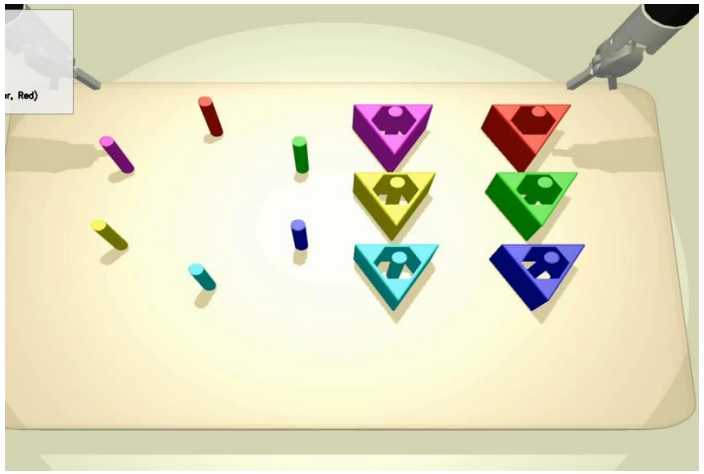


K. Weerasinghe, S. H. Roodabeh, A. Hawkins, Z. Zhang, H. Alemzadeh, "MiDAS: A Multimodal Data Acquisition System for Robot-Assisted Minimally Invasive Surgery," To Appear in *IJMRCAS 2026*.
https://uva-dsa.github.io/MiDAS/

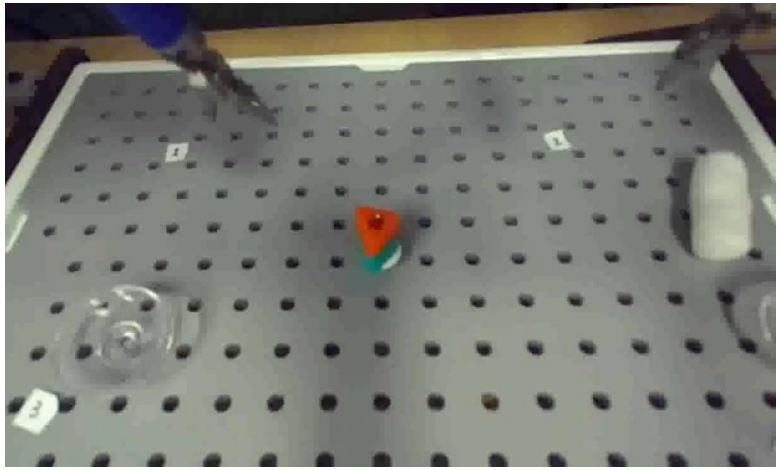
Simulated and Real Procedures

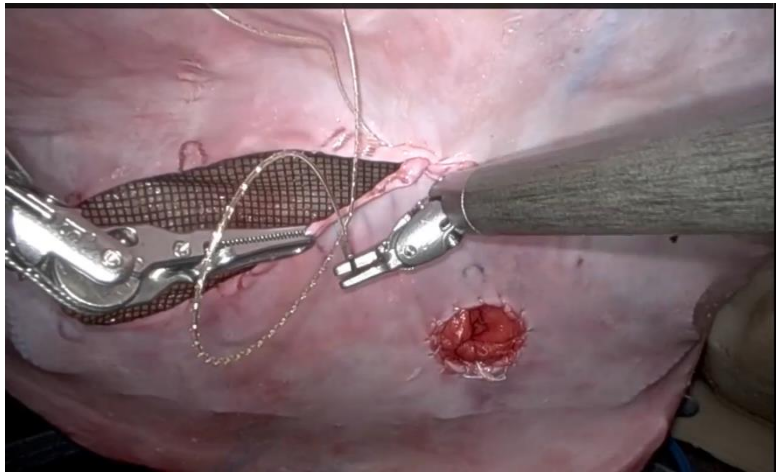
Virtual Reality Simulation



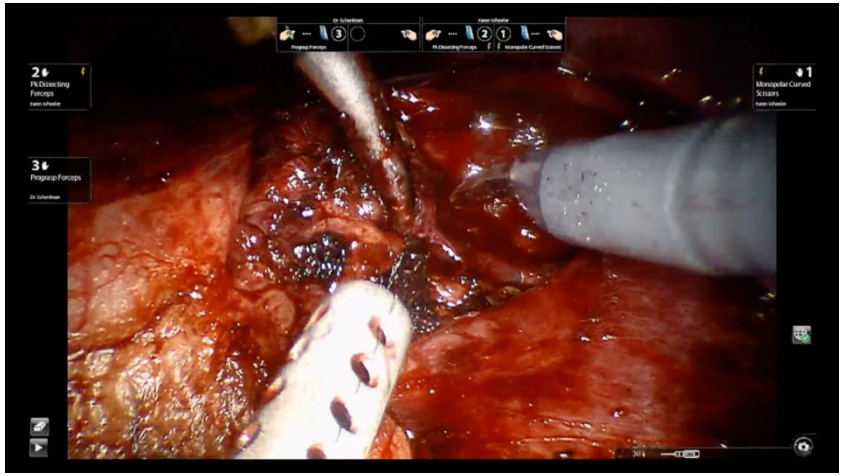


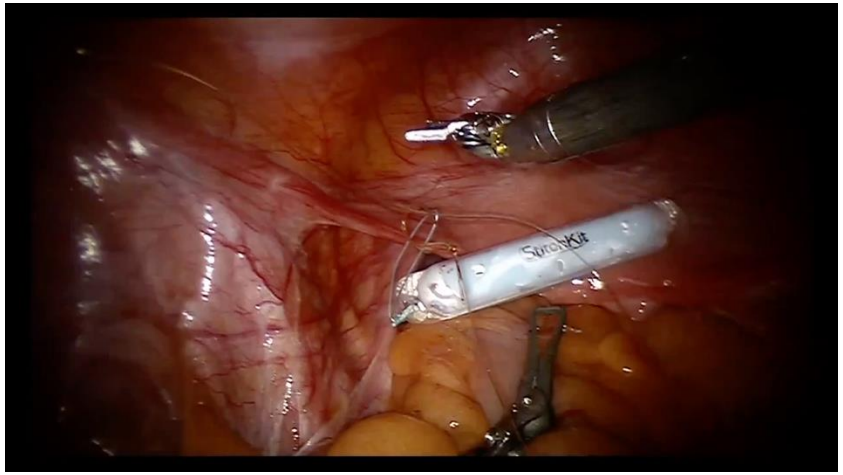
Dry/Wet Lab Simulation

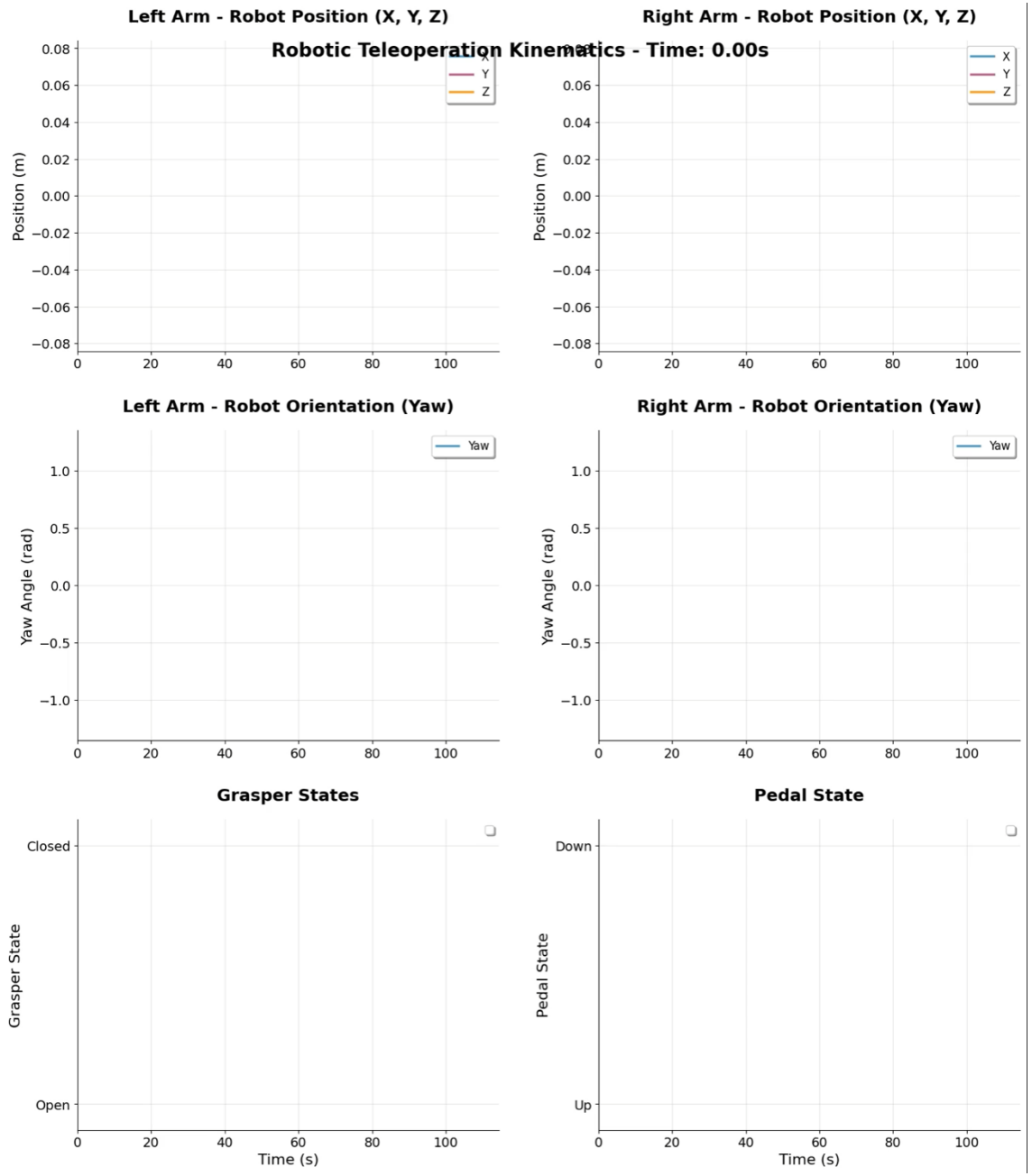


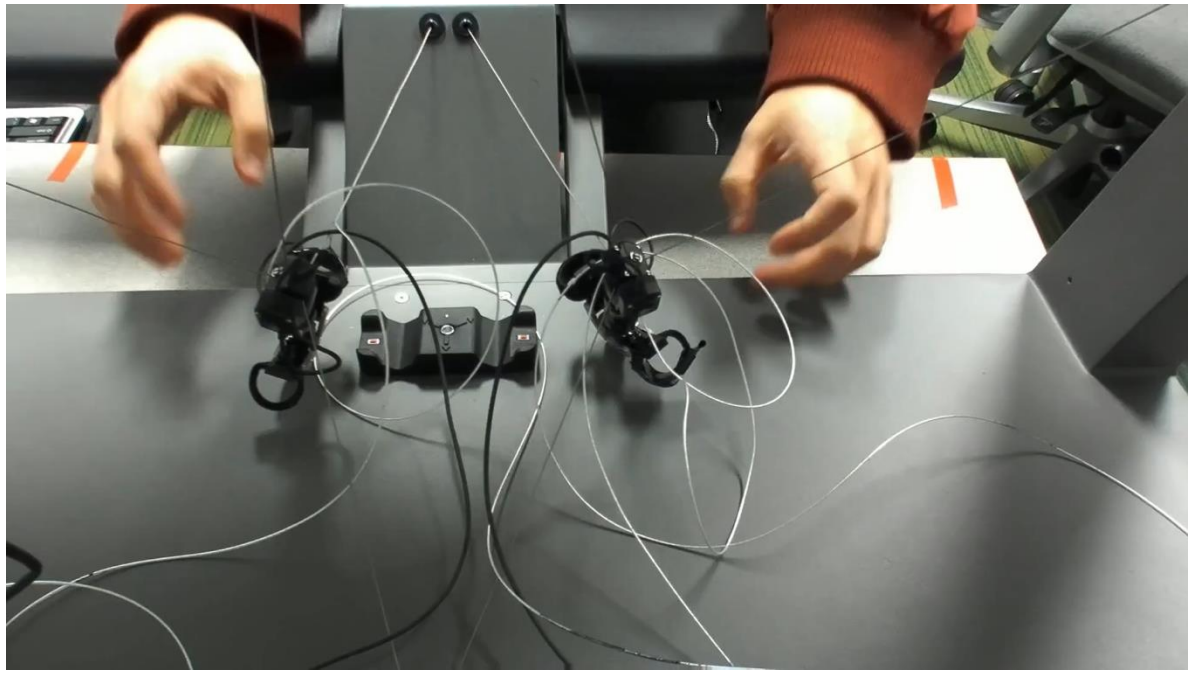


Real Surgery





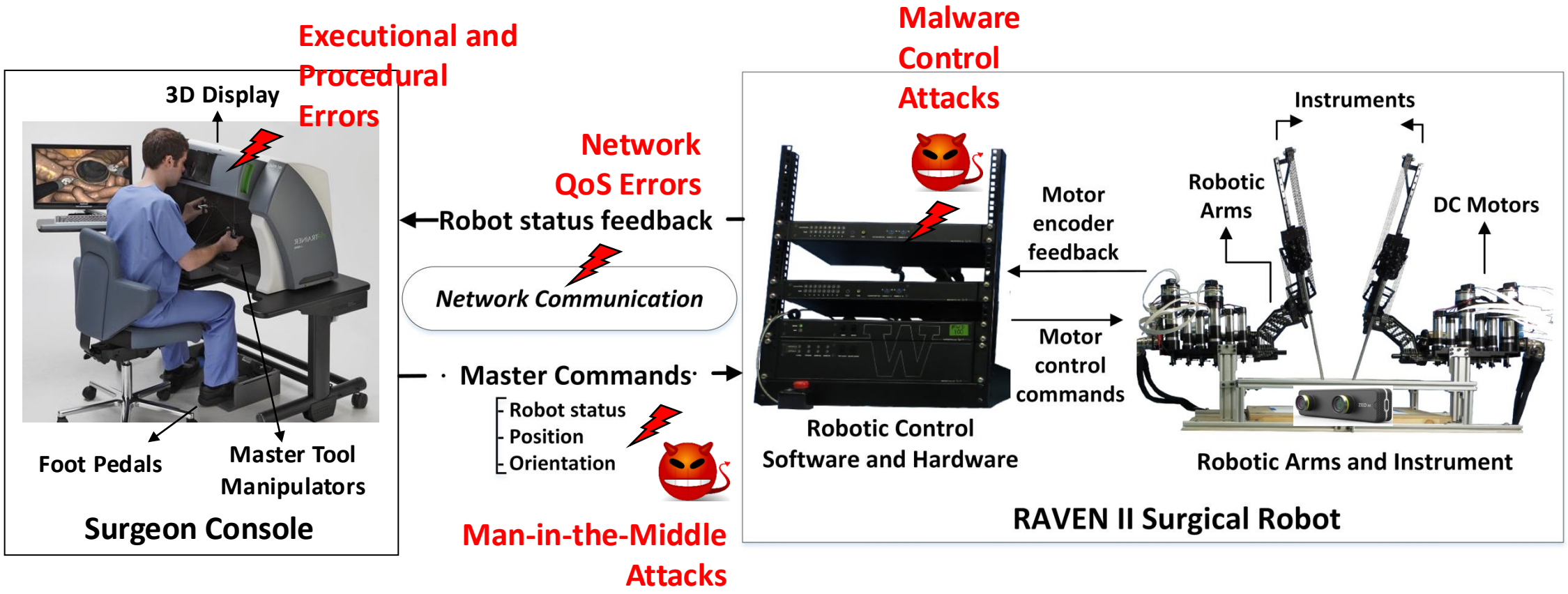




Kinematics, Graspers and Clutch

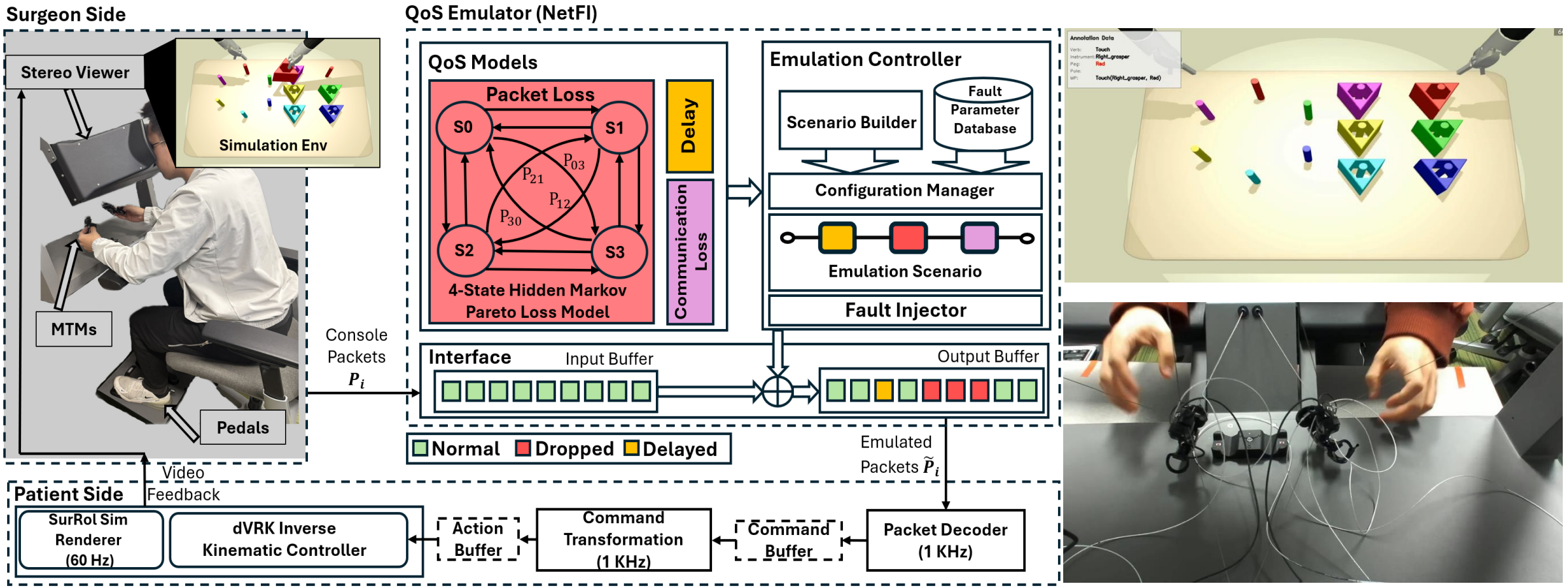
Master Tool Manipulators

Accidental Faults and Malicious Attacks



H. Alemzadeh, *et al.,* "Adverse Events in Robotic Surgery: A Retrospective Study of 14 Years of FDA Data". *PLOS ONE*, 2016.
K. Hutchinson, *et al.,* "Analysis of Executional and Procedural Errors in Dry-lab Robotic Surgery Experiments," *IJMRCAS*, 2022.
H. Alemzadeh, *et al.*, "Targeted Attacks on Teleoperated Surgical Robots: Dynamic Model-Based Detection and Mitigation", *IEEE DSN*, 2016. *(Test of Time Award 2026)*

Network QoS Emulation

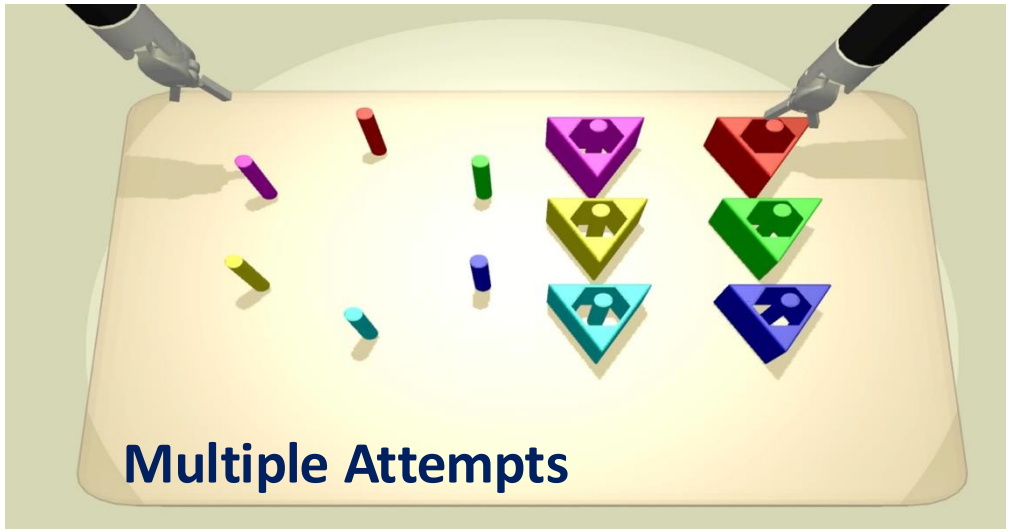


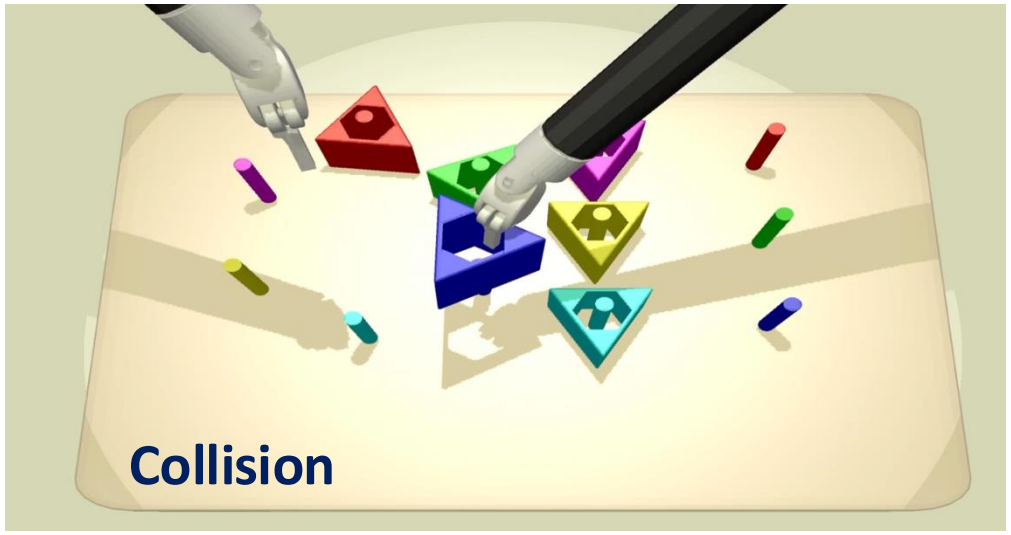
Z. Zhang, *et al.*, "A Comprehensive Analysis of the Effects of Network Quality of Service on Robotic Telesurgery", *ICRA 2026*
https://github.com/UVA-DSA/telesurgery-qos-analysis

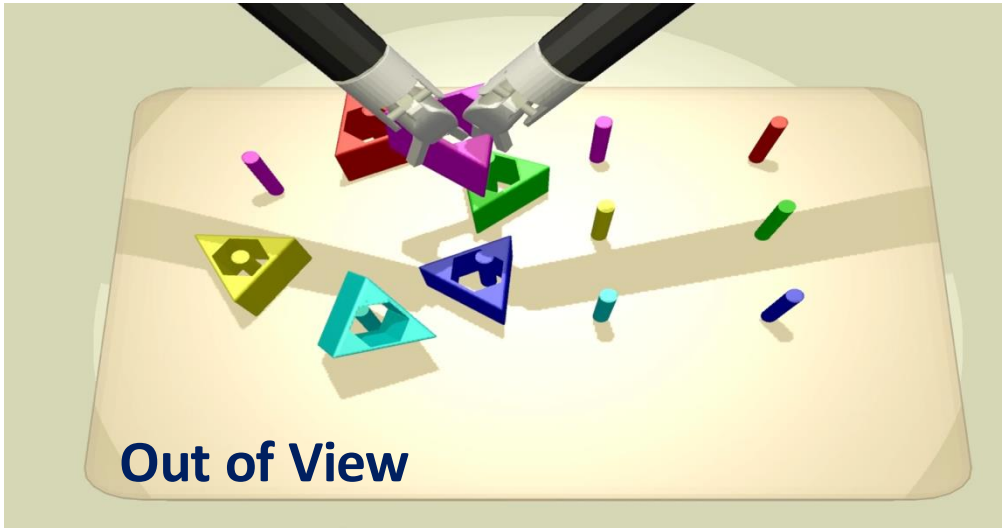
QoS Degradation Scenarios

Degradation Type	Severity	Target	Model Parameters θ
Packet Loss	PLM-1	10% Loss	$\alpha_0 = 4.43, \lambda_0 = 1.64; \alpha_1 = 4.97, \lambda_1 = 0.27$
	PLM-2	30% Loss	$\alpha_0 = 4.60, \lambda_0 = 3.55; \alpha_1 = 3.90, \lambda_1 = 1.47$
	PLM-3	50% Loss	$\alpha_0 = 3.86, \lambda_0 = 3.32; \alpha_1 = 3.80, \lambda_1 = 6.05$
Delay	DLM-1	100 ms	$D_{\min} = 70, w = [.73, .27], \lambda = [.027, .085]$
	DLM-2	300 ms	$D_{\min} = 210, w = [.892, .108], \lambda = [.011, .016]$
	DLM-3	500 ms	$D_{\min} = 406, w = [.895, .105], \lambda = [.010, .015]$
Communication Loss	CLM-1	10% Loss	$L \sim U(0, 3000)\text{ms}, C = 8500\text{ms}$
	CLM-2	30% Loss	$L \sim U(0, 1000)\text{ms}, C = 1000\text{ms}$
	CLM-3	50% Loss	$L \sim U(0, 2000)\text{ms}, C = 1000\text{ms}$

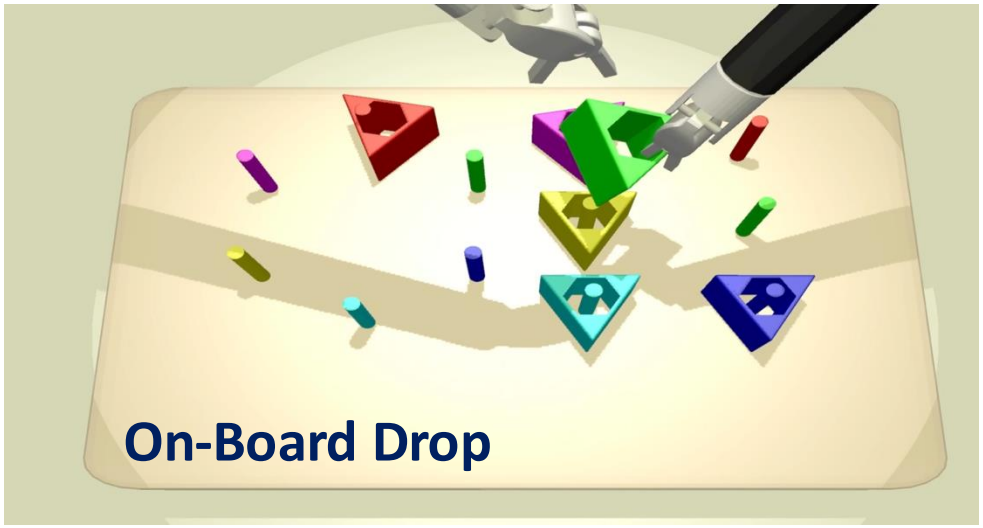
Example Executional Errors





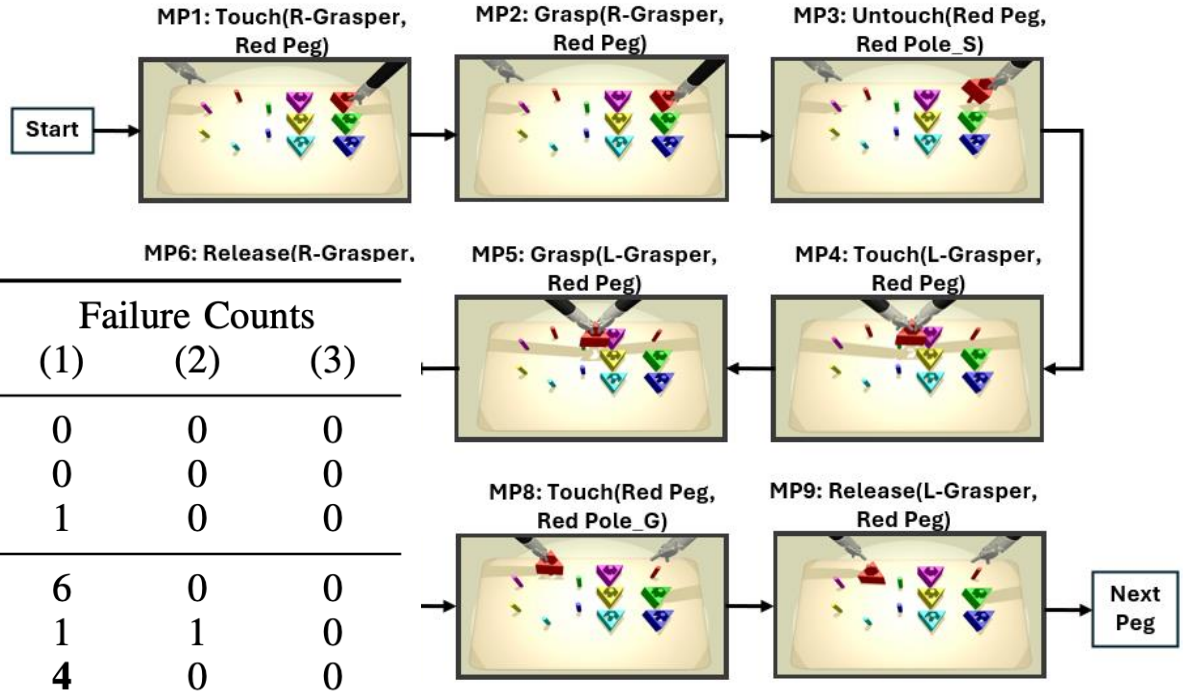


Common Failure Modes



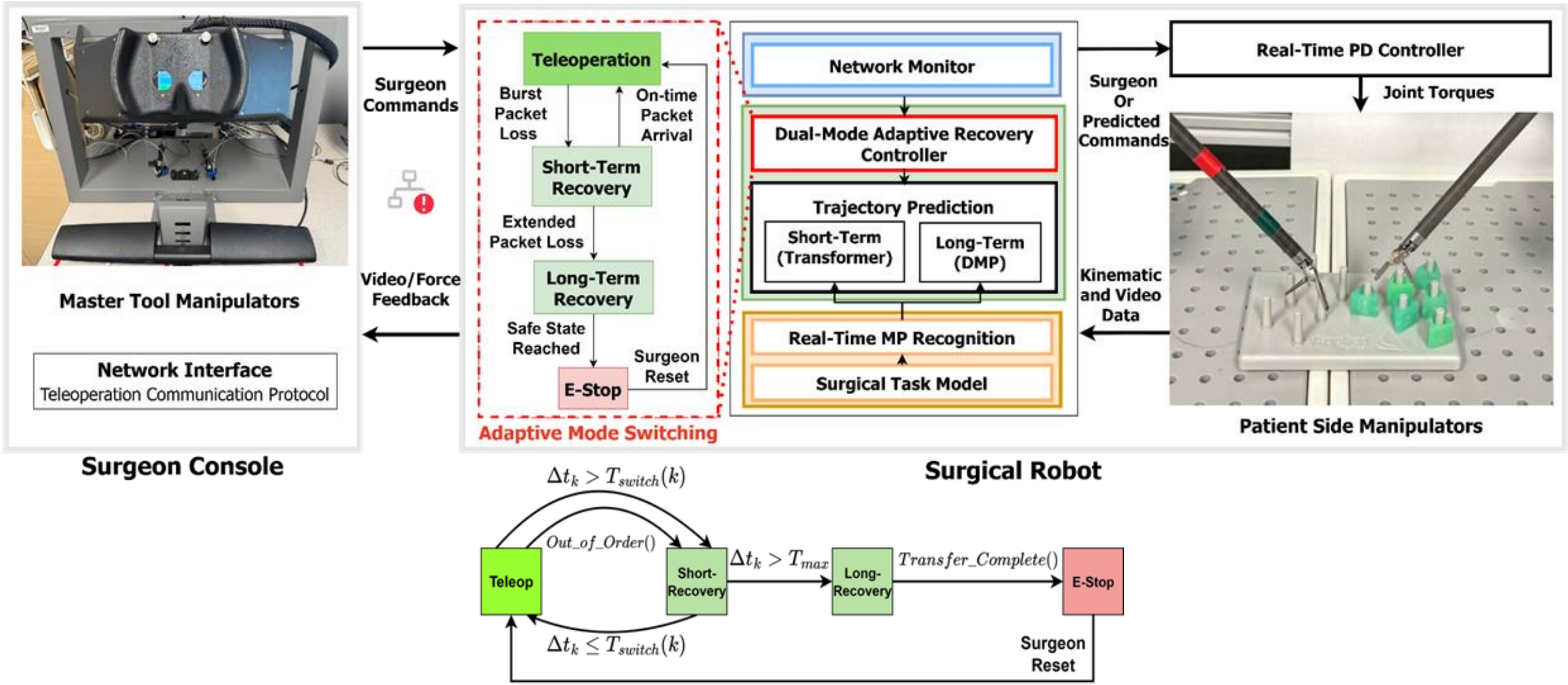
Context-Specific Safety Violations

- **Operational context and errors**
  - Correlation between error types and activities
  - Critical gestures, motion primitives, and errors



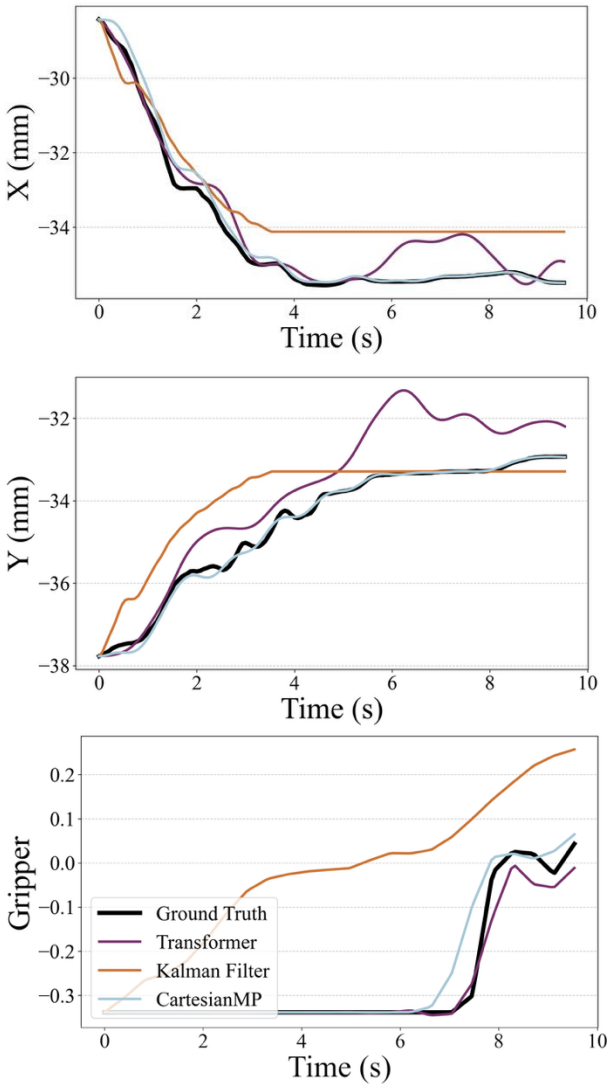
Conditions	Success Rate (%)	Error Counts (1)	(2)	(3)	(4)	Failure Counts (1)	(2)	(3)
Normal-1	100.0 (90/90)	8	3	0	0	0	0	0
Normal-2	100.0 (90/90)	9	6	3	0	0	0	0
Normal-3	98.8 (86/87)	4	6	2	0	1	0	0
PLM-1	93.2 (82/88)	11	12	5	0	6	0	0
PLM-2	97.8 (88/90)	15	5	7	0	1	1	0
PLM-3	95.5 (85/89)	**17**	**11**	**6**	0	**4**	0	0
DLM-1	95.6 (86/90)	6	8	6	0	3	1	0
DLM-2	92.2 (83/90)	13	18	14	2	4	1	2
DLM-3	92.2 (83/90)	**37**	**12**	**26**	0	**5**	0	**2**
CLM-1	100.0 (90/90)	5	9	3	0	0	0	0
CLM-2	95.5 (85/89)	**26**	**21**	**20**	0	**4**	0	0
CLM-3	97.7 (87/89)	13	11	13	0	2	0	0
Most Susceptible MPs		MP1	MP3 & MP4	MP4	MP7	MP4	MP8	MP4

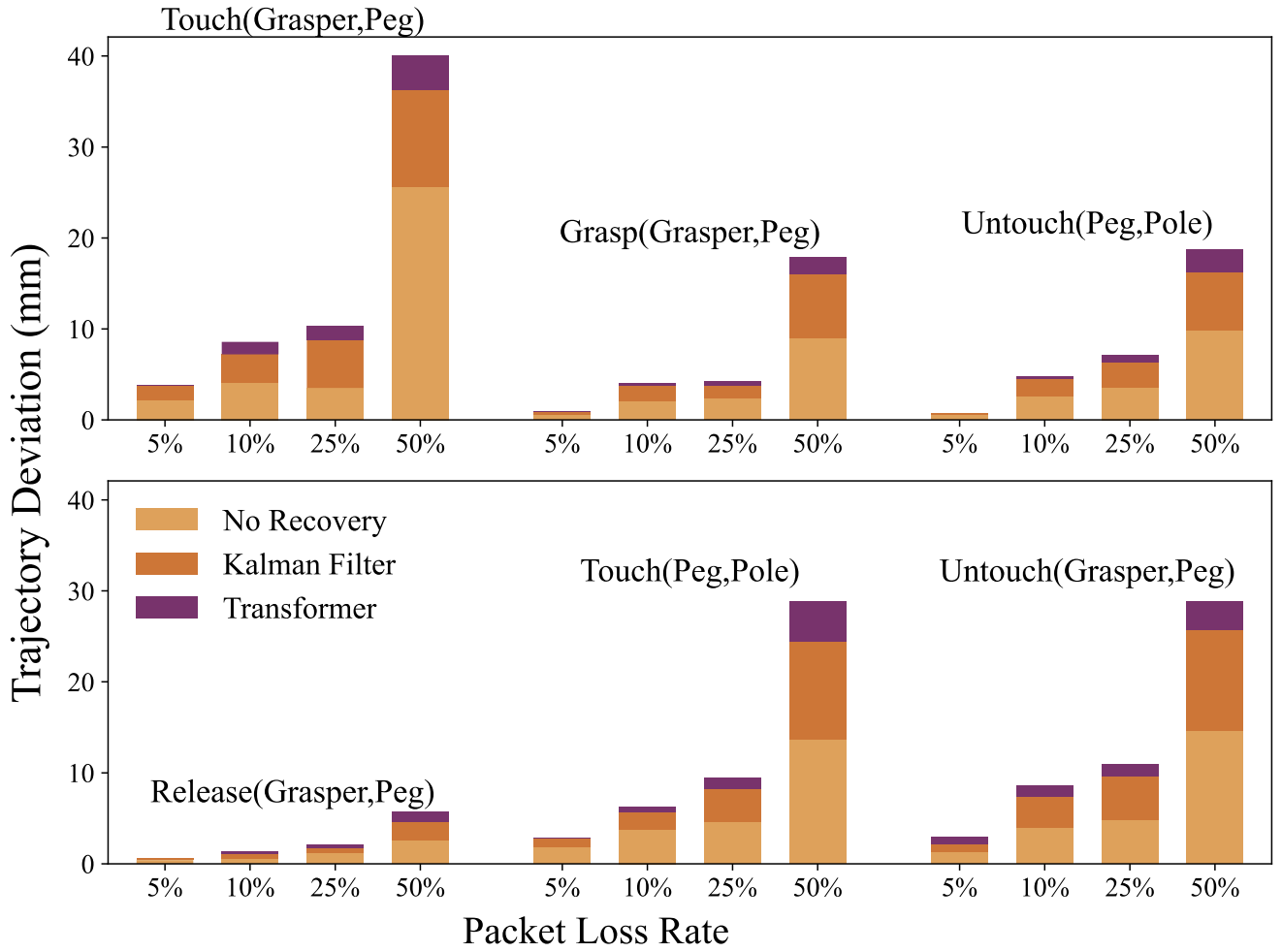
Activity-Aware Error Recovery



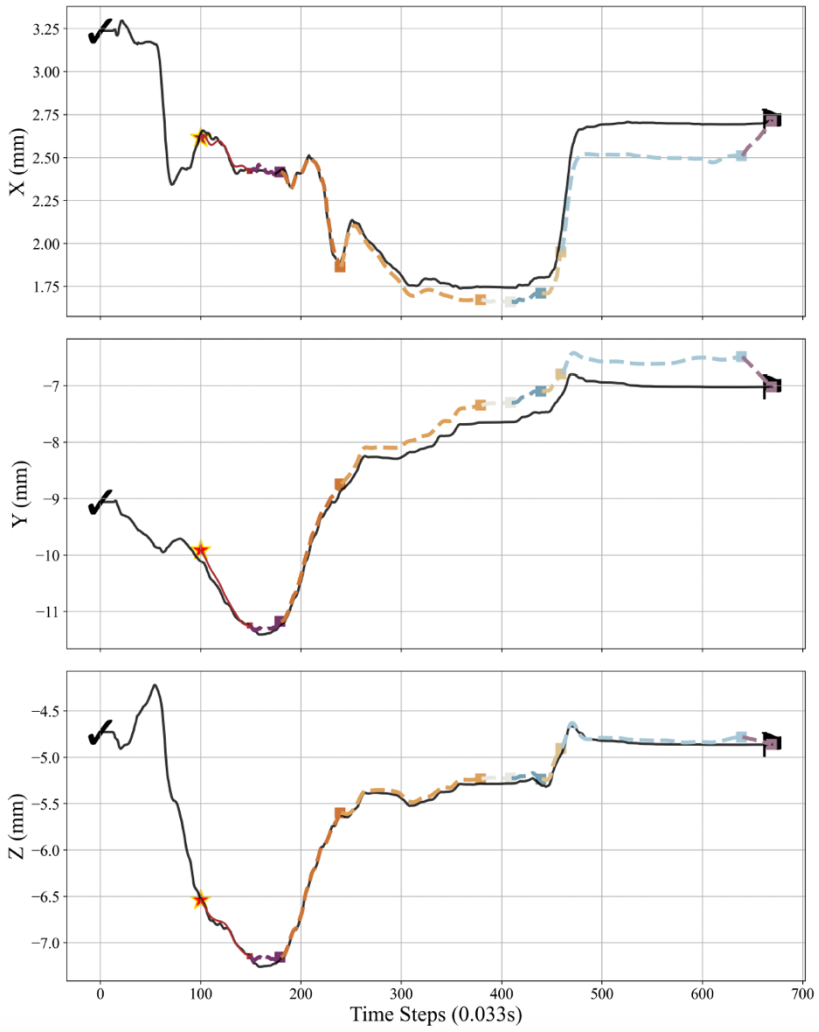
S. H. Roodabeh, H. Alemzadeh, "Activity-Aware Recovery from Network Errors in Tele-operated Robotic Surgery", *Under Review*
https://www.techrxiv.org/doi/pdf/10.36227/techrxiv.176287995.54551665

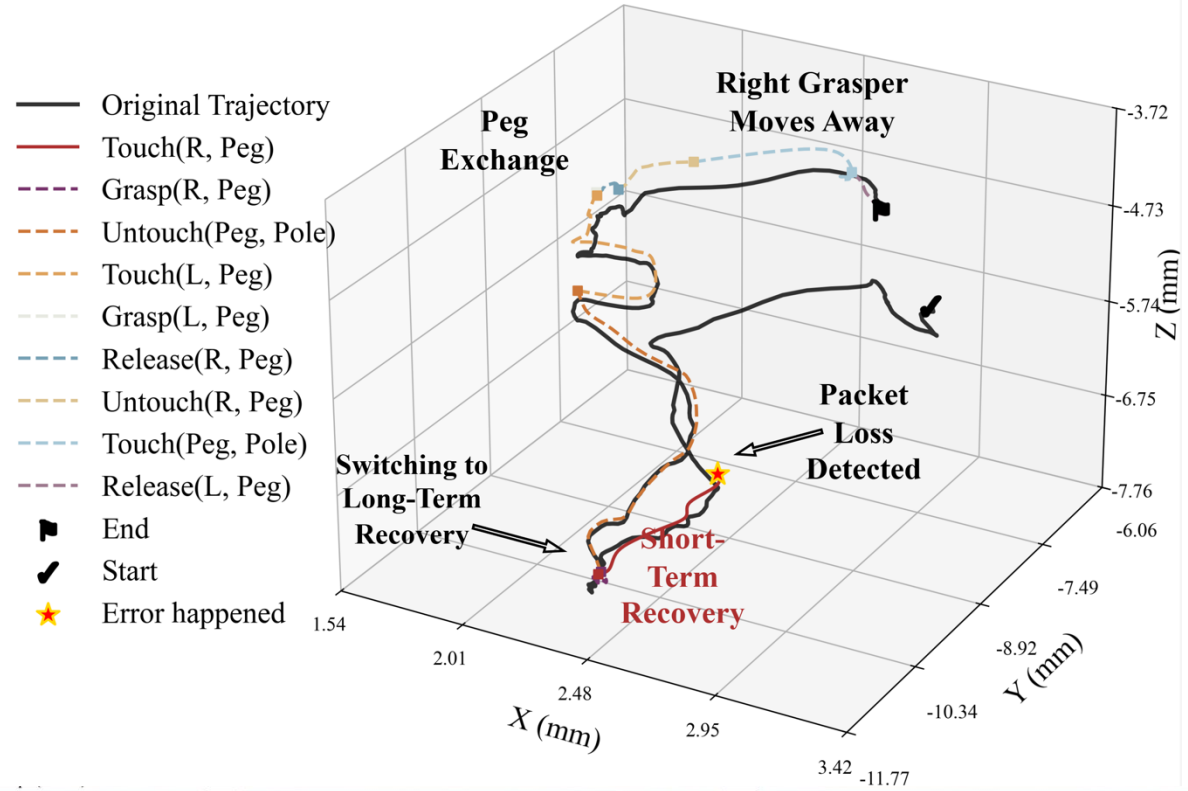
Activity Aware Short-Term Recovery





Activity Aware Dual Mode Recovery






Touch(L-Grasper, Peg)


Unouch(Peg, Pole)


Touch(R-Grasper, Peg)

Future Directions

- Hybrid knowledge and data-driven monitors outperform solely knowledge-based and ML-based monitors, while improving transparency and robustness.
- Context-aware models could facilitate successful hazard mitigation by increasing prediction accuracy and timeliness as well as interpretability.

- Ongoing work:
  - Multimodal data collection and hierarchical labeling (both faulty and fault free)
  - Combined *Human-Cyber-Physical* context modeling, specification and inference
  - *Context-aware* mitigation

- **Testbeds and Datasets on Git:** https://github.com/UVA-DSA/

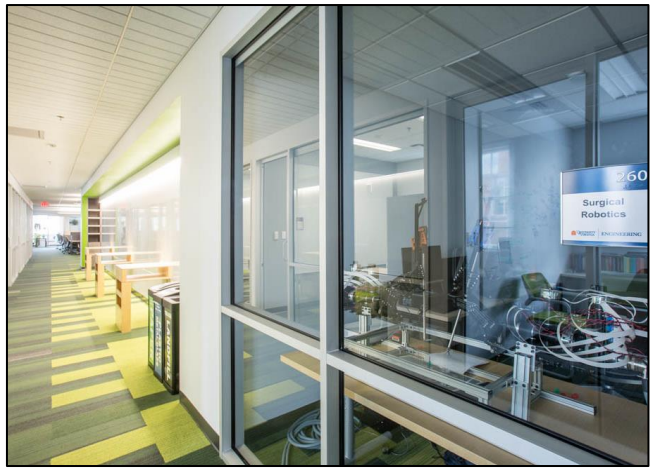
Thank You

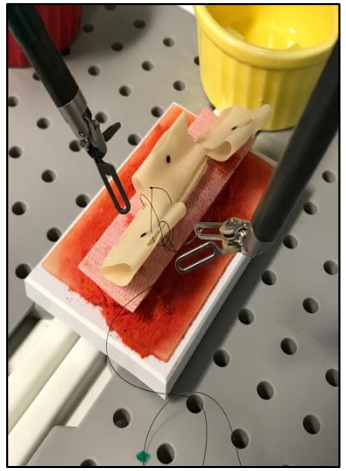
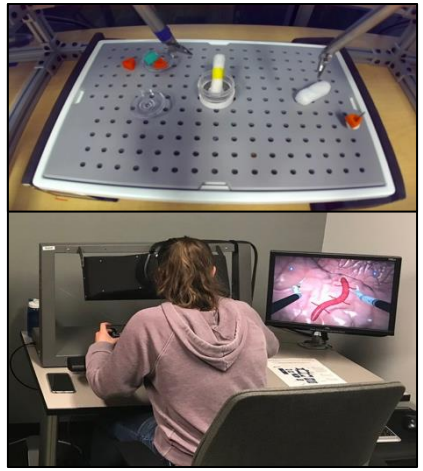
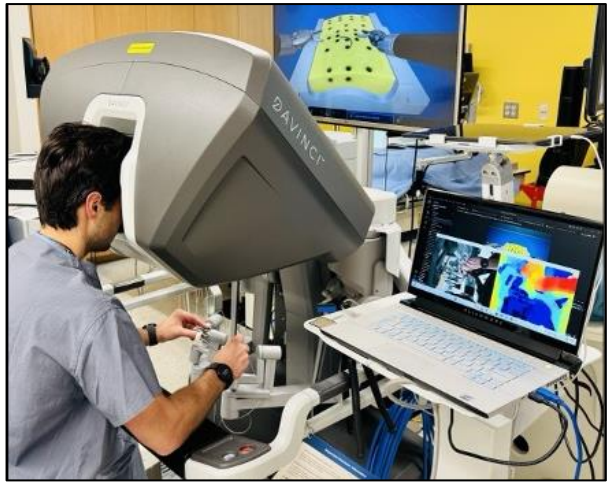




Dependable Systems and Analytics Lab

https://uva-dsa.github.io



UVA DSA LINK LAB

UNIVERSITY of VIRGINIA ENGINEERING

UNIVERSITY of VIRGINIA HEALTH SYSTEM

Commonwealth Cyber Initiative

NIST National Institute of Standards and Technology U.S. Department of Commerce

NSF