Securing Self-Driving Laboratories

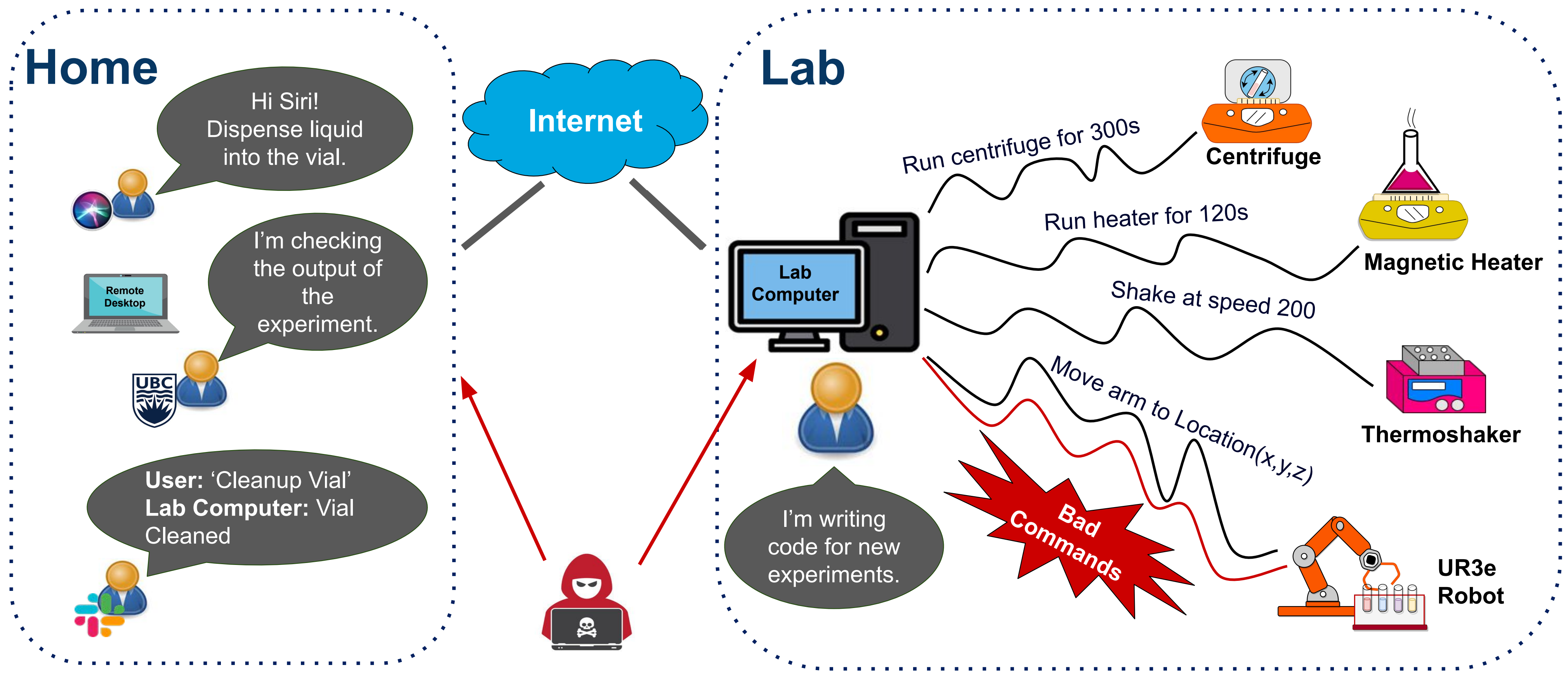
A Collaboration between Computer Science and Chemistry

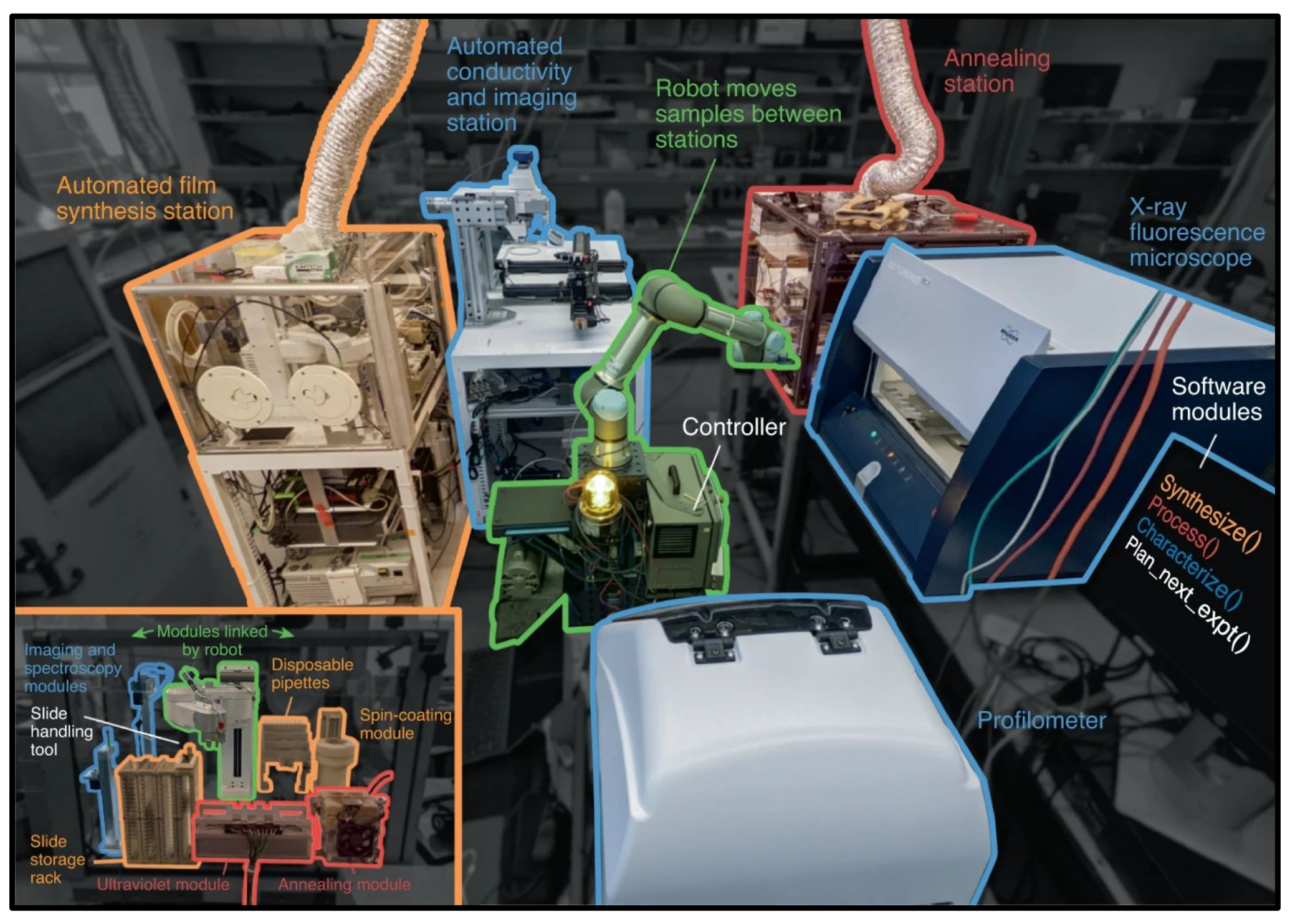
Zainab Saeed Wattoo, Petal Vitis, Arpan Gujarati, Maryam Aliabadi, Sean Clark, Noah Depner, Xiaoman Liu, Parisa Shiri, Amee Trivedi, Ivory Zhang, Ruizhe Zhu, Jason Hein, and Margo Seltzer

1 Attacks on Cyber-Physical Systems Cause Real-World Physical Damage

Example: Hein Lab, Blending Advanced Robotics with Synthetic Organic Chemistry

“Accelerating the rate of research and discovery by integrating these instruments with autonomous robotics to develop self-driving laboratories.”


Home
Hi Siri! Dispense liquid into the vial.
Remote Desktop
I’m checking the output of the experiment.
UBC
User: ‘Cleanup Vial’ Lab Computer: Vial Cleaned
Internet
Lab
Lab Computer
I’m writing code for new experiments.
Run centrifuge for 300s
Centrifuge
Run heater for 120s
Magnetic Heater
Shake at speed 200
Thermoshaker
Move arm to Location(x,y,z)
Bad Commands
UR3e Robot

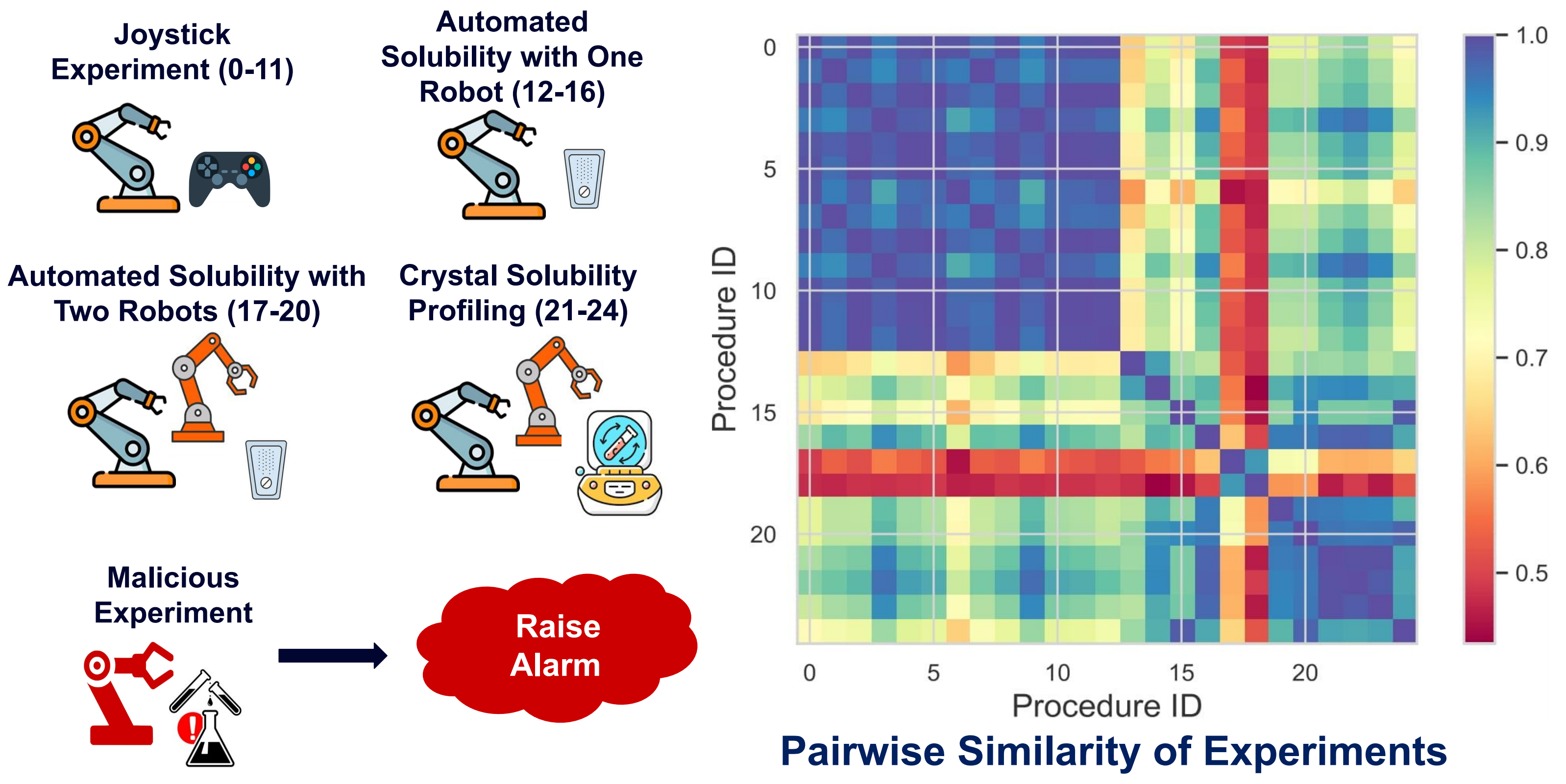


Threat: Malicious commands sent to robot arms and smart devices, which could harm people in the lab

2 Using Command History and Domain Knowledge to Detect Intrusions

Prior Work

Data tracing, collection, and preliminary analysis (DSN’22)



Pairwise Similarity of Experiments

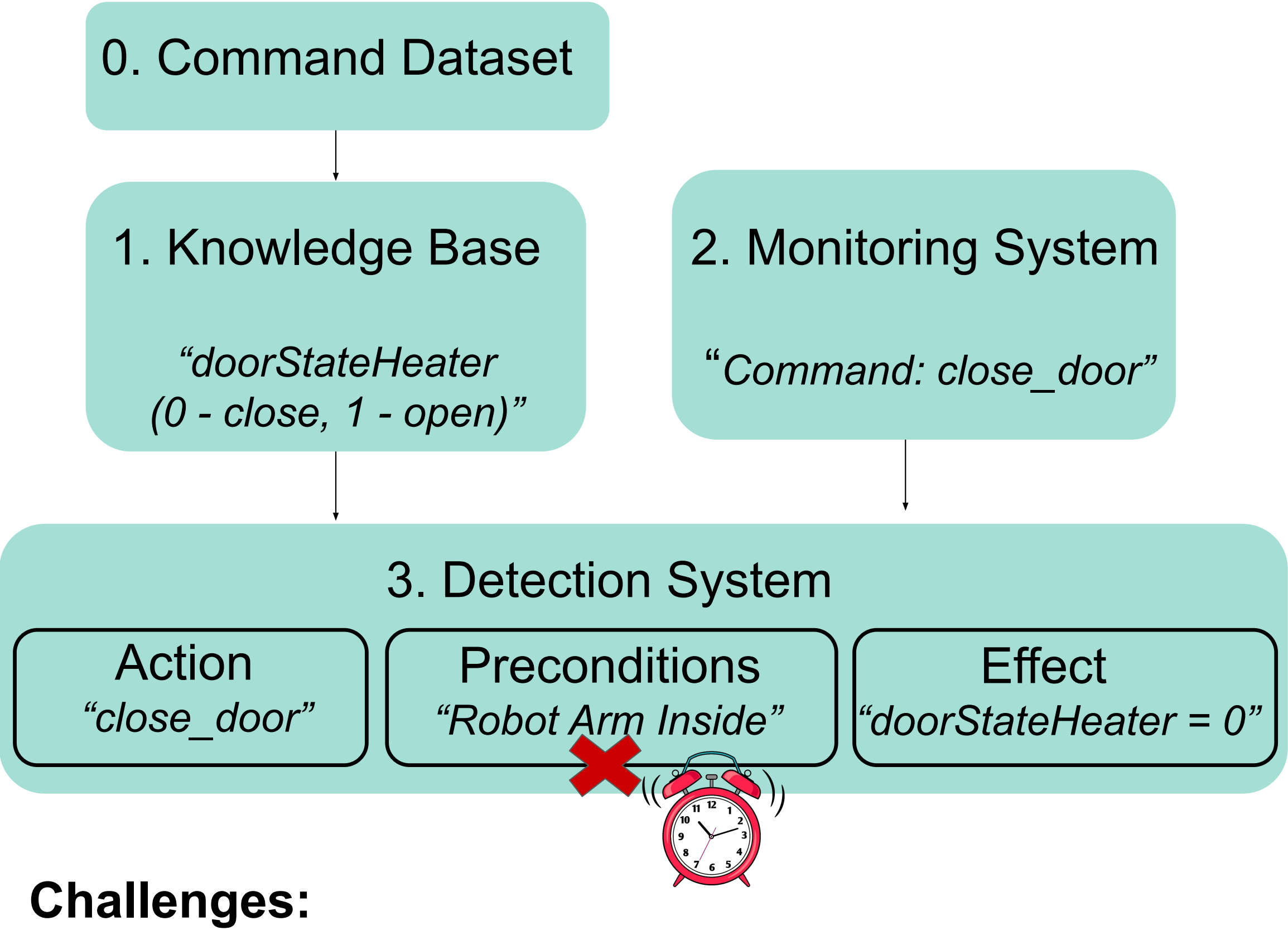
Observation: Command dataset could be used to infer underlying identifiable patterns

Current Work

Rule-Based Intrusion Detection System (IDS)

Set of General Rules
Do not heat an empty test tube.
Do not pick up an object if the robot arm is already holding something.
Do not put the material in the vial if it exceeds its capacity.
Do not close the door of the device if the robot arm is inside the device.
Do not move the robot arm to a a location if it is occupied by an object.

Set of Hein-Lab Specific Rules
Do not add liquid before the solid in a vial.
Do not place the vial on the centrifuge if it does not contain both solid and liquid.
Do not place the vial inside the centrifuge if the red dot on the centrifuge does not face North.



0. Command Dataset

1. Knowledge Base
“doorStateHeater (0 - close, 1 - open)”

2. Monitoring System
“Command: close_door”

3. Detection System

Action	Preconditions	Effect
“close_door”	“Robot Arm Inside”	“doorStateHeater = 0”

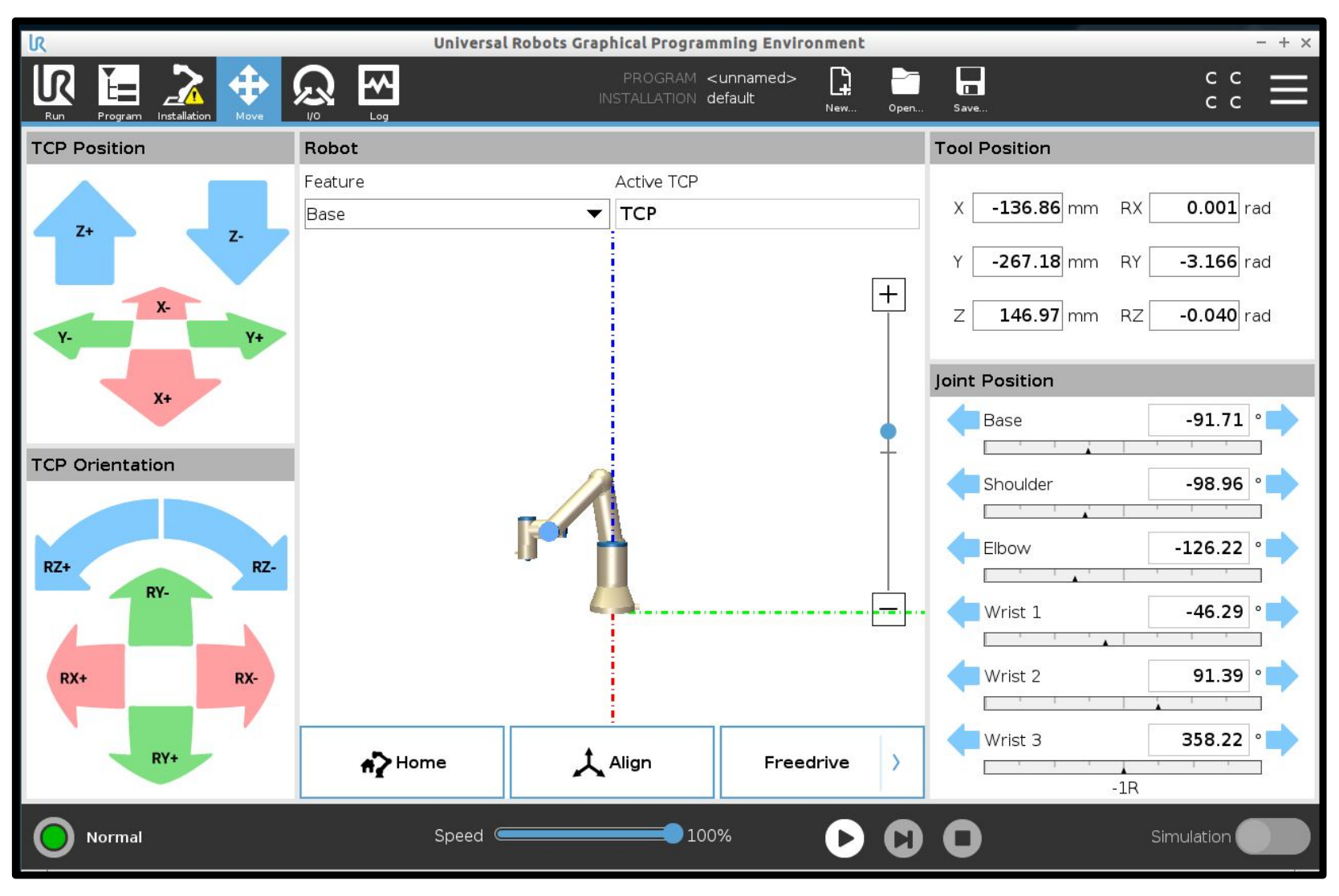
Challenges:

- Automating synthetic organic chemistry is a new domain
- Heterogeneous devices
- Formalizing an exhaustive set of rules
- The CPS platform and experiments are dynamic

3 Evaluation Methodology: Intrusion Detection using a Three-Step Approach

1 Enhanced Simulator

Allows for in-house testing without physical access to the robot arm



PROGRAM <unnamed>
INSTALLATION default

TCP Position

TCP Orientation

Robot
Feature: Base
Active TCP: TCP

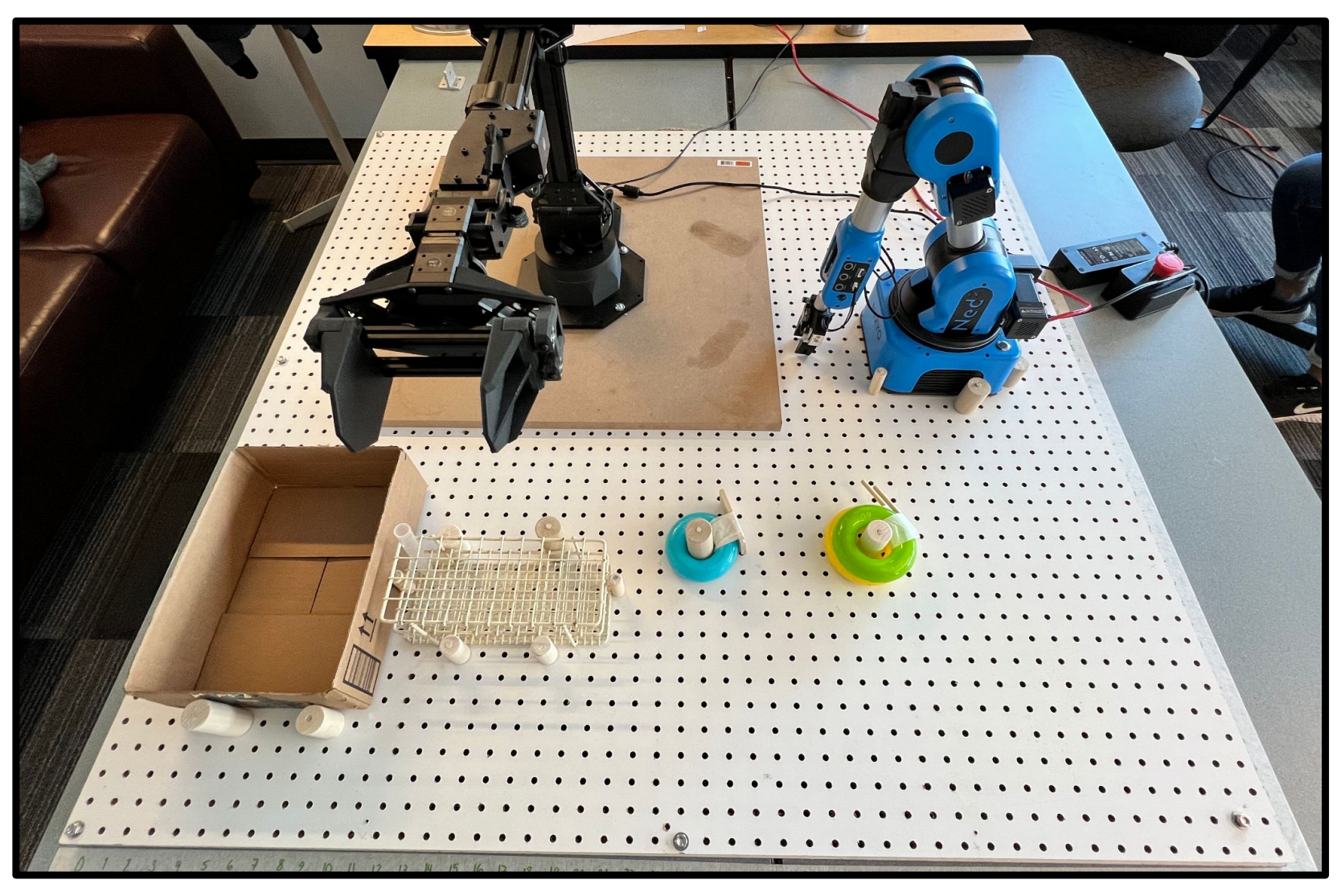
Tool Position
X -136.86 mm RX 0.001 rad
Y -267.18 mm RY -3.166 rad
Z 146.97 mm RZ -0.040 rad

Joint Position
Base -91.71 °
Shoulder -98.96 °
Elbow -126.22 °
Wrist 1 -46.29 °
Wrist 2 91.39 °
Wrist 3 358.22 °
-1R

Speed 100%

2 Test Bed

Allows for testing scenarios that span multiple robot arms



3 Hein Lab

Allows for evaluation of all robotic arms and smart devices at production level