Modeling Human-Cyber Interactions in Safety-Critical Cyber-Physical/Industrial Control Systems (CPS/ICS)

Steven Ngo[1], Luis Garcia[2], Dave DeAngelis[2]

[1]California Polytechnic State University, San Luis Obispo, [2]University of Southern California, Information Sciences Institute

Work performed under REU Site program supported by NSF grant #2051101

Motivation

- **Human mistakes and insider threats** within the CPS/ICS industry often put lives at stake due to the safety-critical nature, in addition to the cost of millions of dollars for damages and repairs.
- Current state of the CPS research community involves a lot of work on the systems-side, but there is a **lack of consideration for the human element** (e.g., operators, network users).
- Industry 4.0 marks a shift to a stronger integration between humans and machine, including human-CPS, but it can be **difficult to effectively map out human behavior** for research purposes.

RQ: How can we model and simulate realistic human behavior in cyber-physical systems?

Background

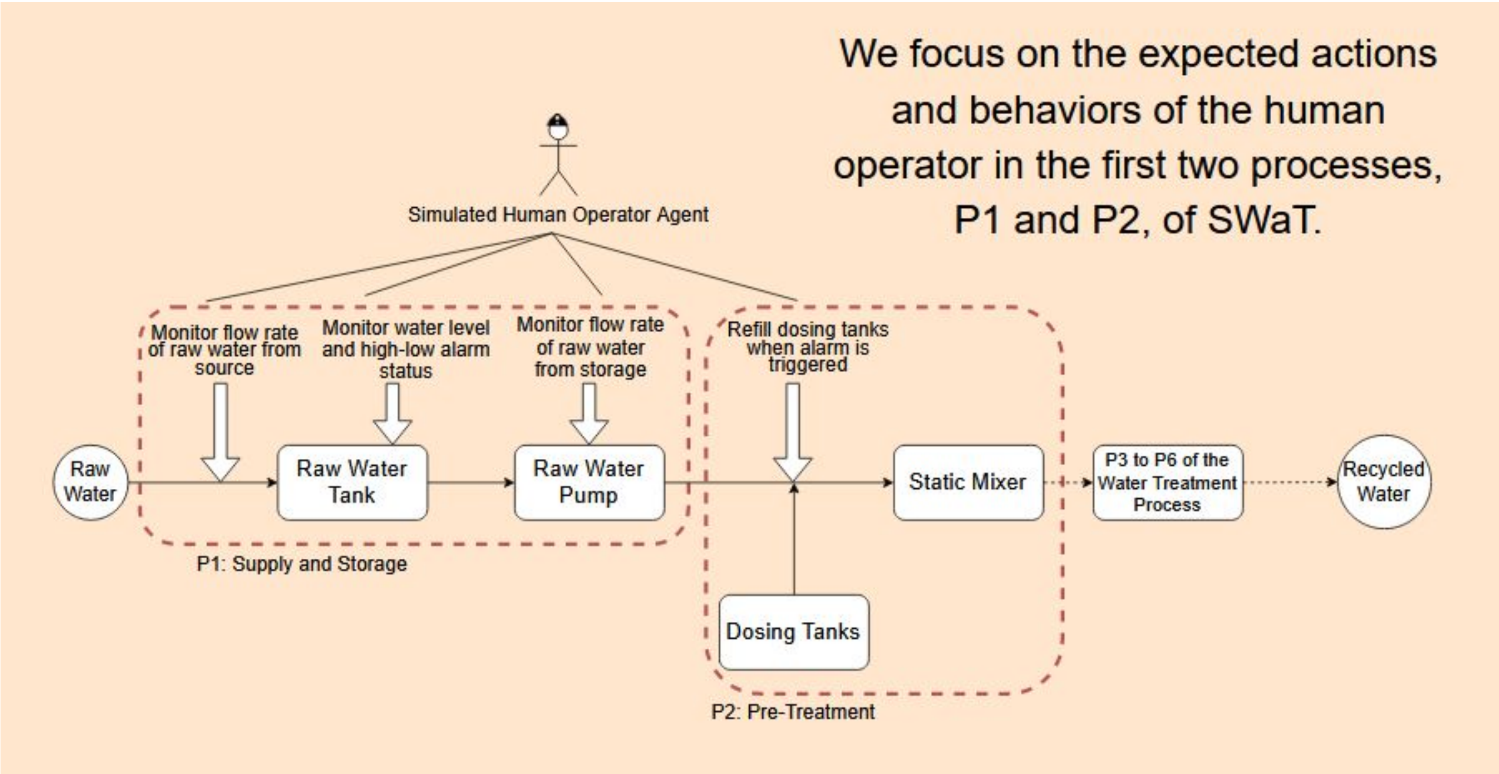
Areas of Interest

- *CPS Modeling and System Analysis*
  - Current work focuses on modeling to counter external threats and attacks that hop through multiple system components, and human aspects are often abstracted to be definitive.
- *Anomaly and Threat Detection*
  - Some CPS intrusion detection systems (IDS) are behavior-specification-based, where a formal specification of the system is provided, and the IDS picks up on "non-legitimate" behavior.
- *Modeling Human Behavior in Security Context*
  - One way to model human behavior is to consider both a rational and instinctive approach to how we make decisions.[1]
  - Our thought process and current knowledge (mental models) power the rational behavior, while our subconsciousness drives the instinctive behavior.

Contributions

- We offer a **novel technique of modeling human behavior**, starting with decision-making, in CPS/ICS research.
- We present a **use case of our process**, utilizing DASH human models and SWaT (water treatment testbed) with support from MiniCPS, that serves as a proof-of-concept.

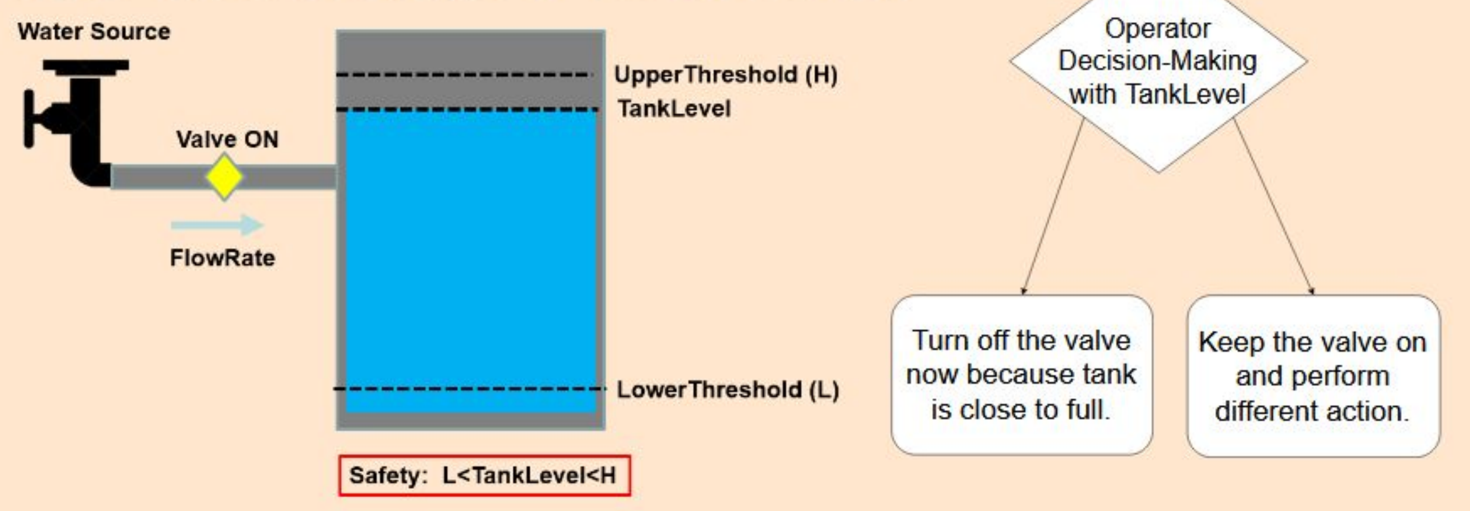
Use Case: Human-Cyber SWaT Model



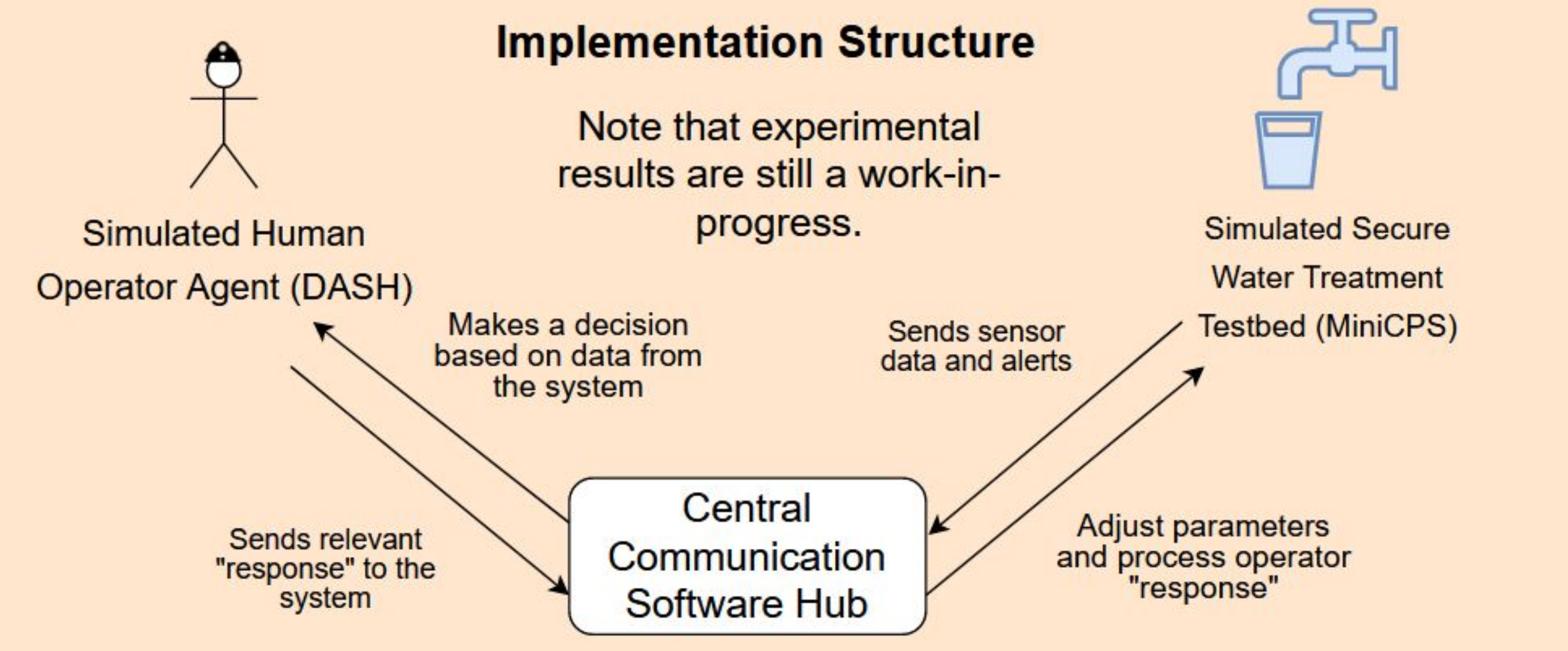
We focus on the expected actions and behaviors of the human operator in the first two processes, P1 and P2, of SWaT.

Simulated Human Operator Agent
Monitor flow rate of raw water from source
Monitor water level and high-low alarm status
Monitor flow rate of raw water from storage
Refill dosing tanks when alarm is triggered
Raw Water
Raw Water Tank
Raw Water Pump
Static Mixer
P3 to P6 of the Water Treatment Process
Recycled Water
Dosing Tanks
P1: Supply and Storage
P2: Pre-Treatment

Example Scenario: Does the operator shut off the valve when it is *close* to the threshold?



Water Source
Valve ON
FlowRate
UpperThreshold (H)
TankLevel
LowerThreshold (L)
Safety: L<TankLevel<H
Operator Decision-Making with TankLevel
Turn off the valve now because tank is close to full.
Keep the valve on and perform different action.

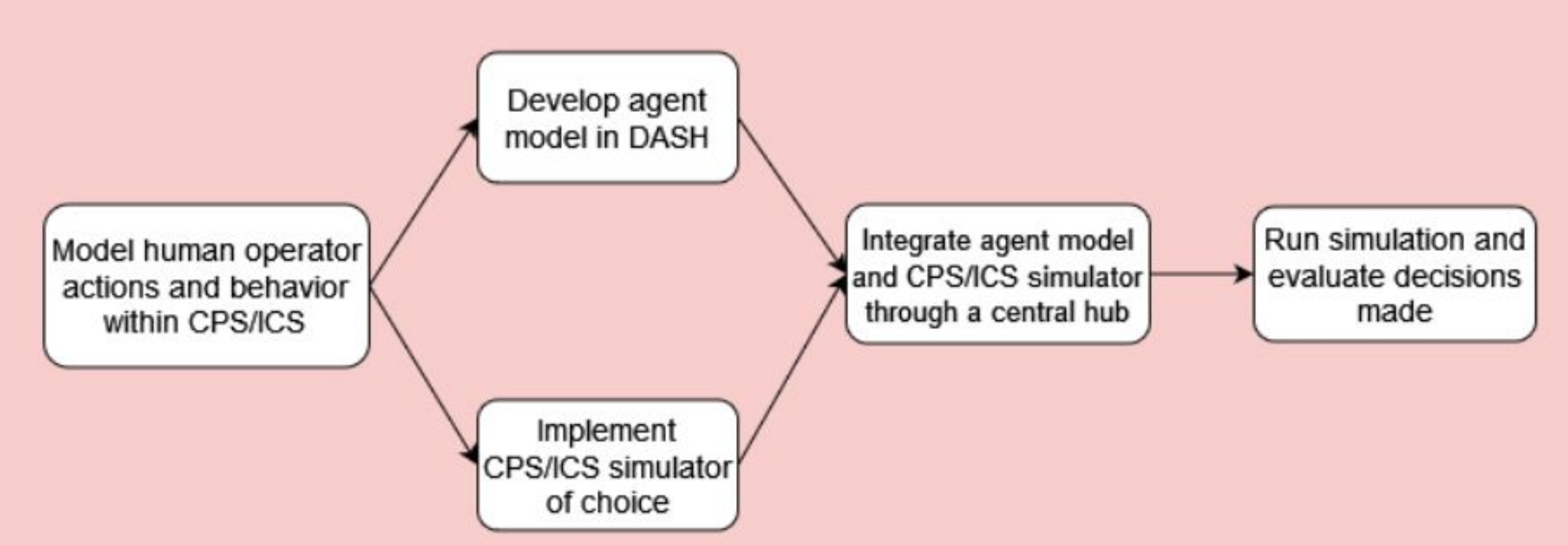


Implementation Structure

Note that experimental results are still a work-in-progress.

Simulated Human Operator Agent (DASH)
Simulated Secure Water Treatment Testbed (MiniCPS)
Makes a decision based on data from the system
Sends sensor data and alerts
Central Communication Software Hub
Sends relevant "response" to the system
Adjust parameters and process operator "response"

Process Overview



Model human operator actions and behavior within CPS/ICS
Develop agent model in DASH
Implement CPS/ICS simulator of choice
Integrate agent model and CPS/ICS simulator through a central hub
Run simulation and evaluate decisions made

Challenges

- Almost impossible to develop an agent model that factors in every possible behavior/decision, so we need to limit it to core processes.
- We need to validate simulation data against ground truth data acquired from evaluating the decisions made by actual humans.

Relevant Frameworks

- *DASH – Deterlab Agent Simulating Humans*[1]
  - Human behavior-modeling framework with a dual-process cognitive architecture (rational and instinctive behavior).
  - We use this framework in creating our simulated CPS human operator agent.
- *MiniCPS*[2]
  - CPS real-time simulating framework.
  - We use this framework to simulate Singapore University of Technology and Design's Secure Water Treatment (SWaT) testbed.

Future Work

- Design method to acquire ground truth data and compare.
- Integrate human-cyber interactions into system formal integrations for behavior-specification-based IDS.
- Explore additional use cases, including UAVs and other types of ICS.

1 - J. Blythe, "A dual-process cognitive model for testing resilient control systems," *2012 5th International Symposium on Resilient Control Systems*, 2012, pp. 8-12, doi: 10.1109/ISRCS.2012.6309285.

2 - Daniele Antonioli and Nils Ole Tippenhauer. 2015. MiniCPS: A Toolkit for Security Research on CPS Networks. In Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy (CPS-SPC '15). Association for Computing Machinery, New York, NY, USA, 91–100. https://doi.org/10.1145/2808705.2808715