

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

Steven Ngo (CP SLO), Luis Garcia (ISI), Dave DeAngelis (ISI)

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

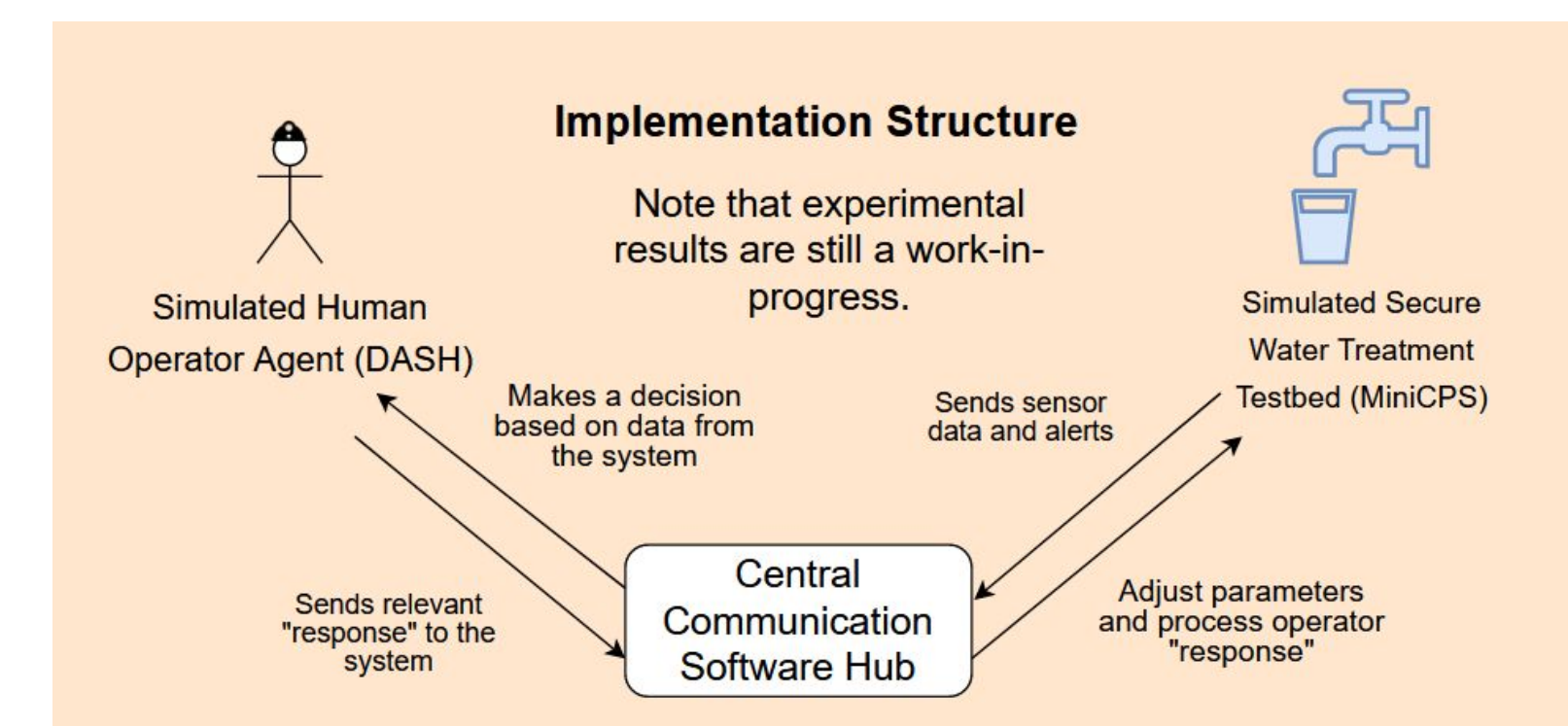
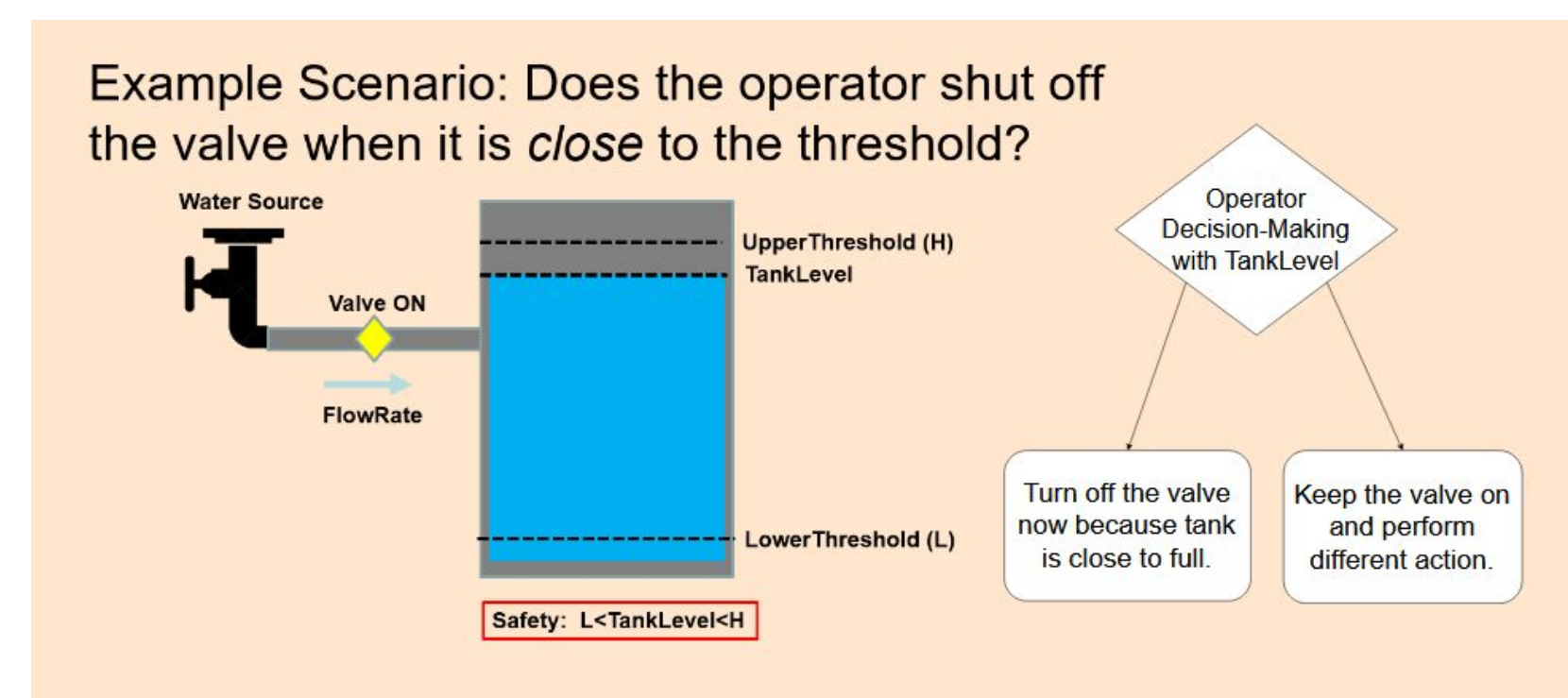
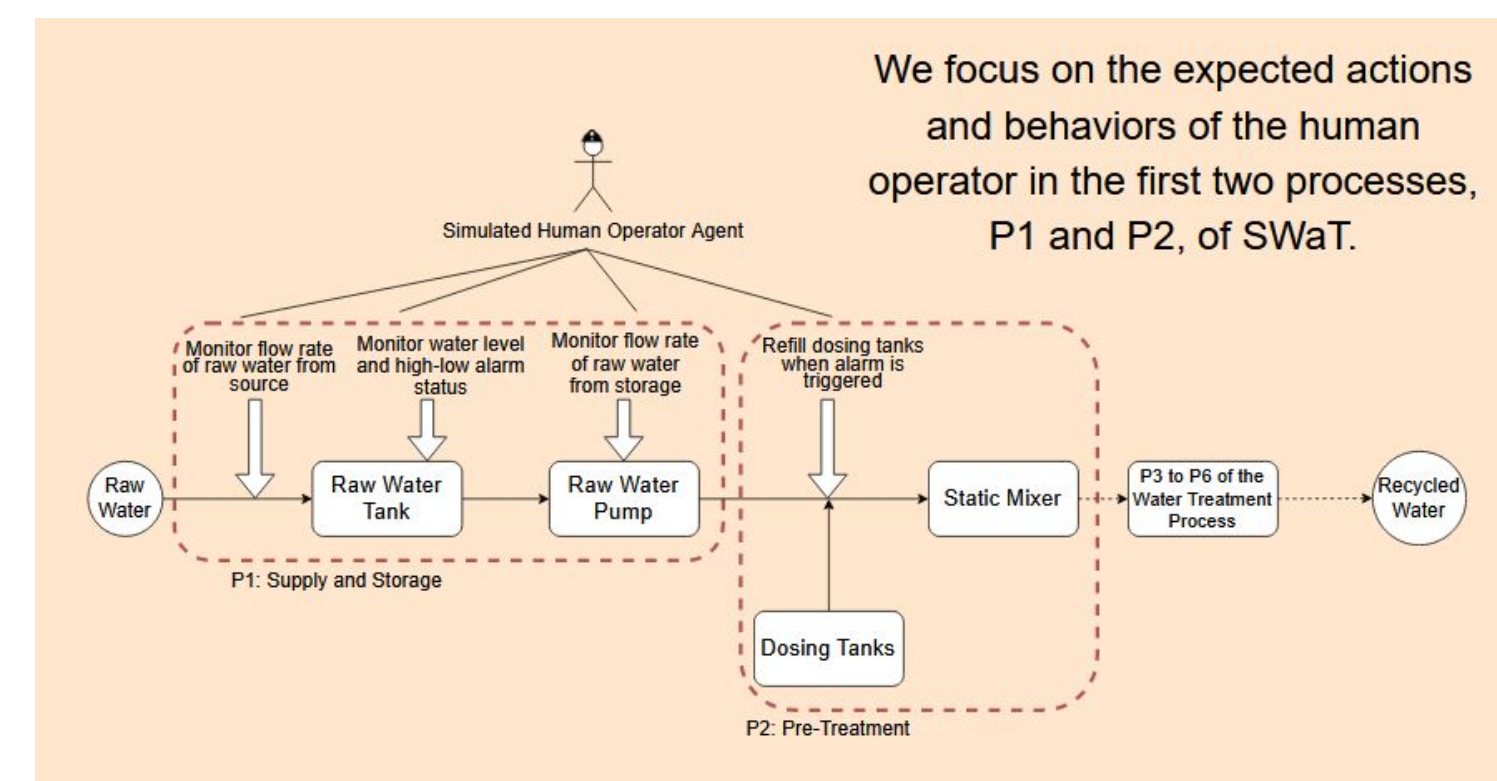
Areas of Interest

- ❖ **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.

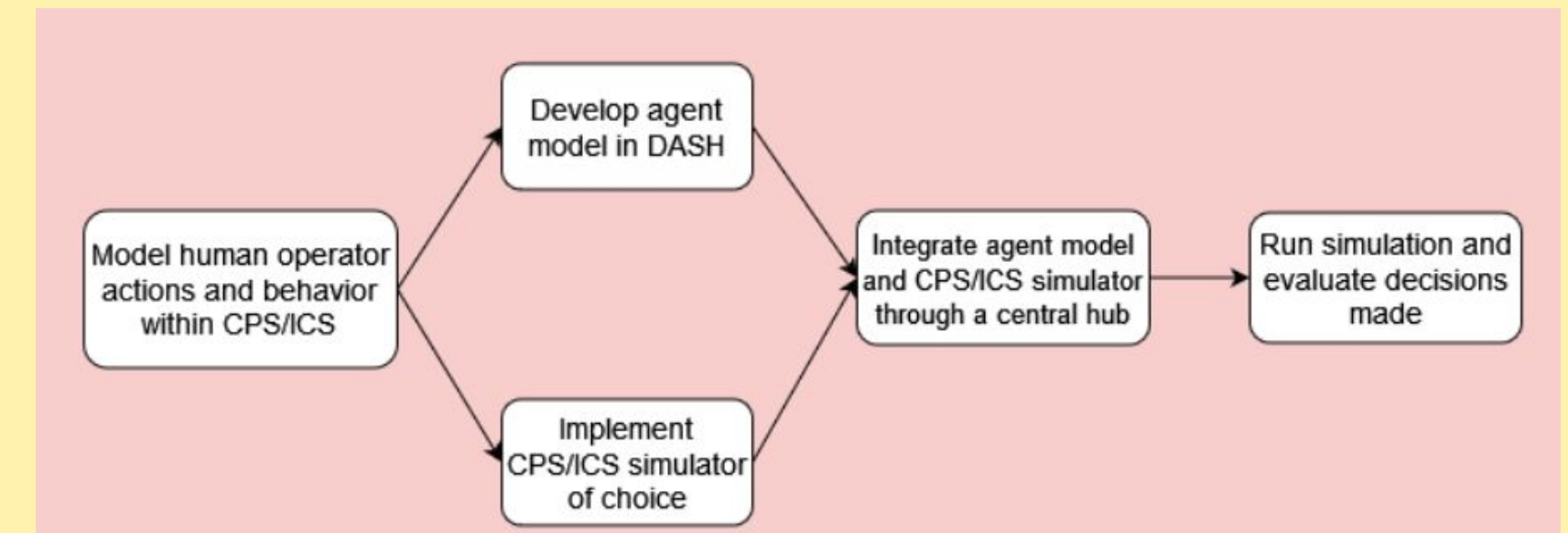
Contributions

- ❖ 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



Process Overview



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>