Modeling Human-Cyber Interactions in Safety-Critical Cyber-Physical/Industrial Control Systems

Steven Ngo
California Polytechnic State University, San Luis Obispo
San Luis Obispo, California, USA
sngo12@calpoly.edu

Dave DeAngelis, Luis Garcia
Information Sciences Institute
University of Southern California
Marina del Rey, California, USA
deangeli@isi.edu, lgarcia@isi.edu

***Abstract*—Safety-critical cyber-physical and industrial control systems (CPS/ICS) such as electrical power grids and water treatment plants are prone to external attacks and internal mistakes or threats. Still, research in this area does not involve high-fidelity human models in their CPS state estimation models. We provide a starting point to modeling the expansiveness of human behavior in CPS by proposing Cyber-Human Interaction Modeling for Cyber-Physical Systems (CHIMPS), a novel decision-making-based process to explicitly integrate human models in the design and implementation of CPS. We present a use case of our process focusing on safety-critical ICS that simulates a human ICS operator maintaining a water treatment plant.**

***Index Terms*—cyber-physical systems, industrial control systems, system state estimation, human-computer interaction**

I. Introduction

Cyber-physical systems (CPS) combine physical processes with computational power through embedded computers and networks to create complex control systems throughout various application domains across homes and workplaces. Safety-critical CPS, mainly industrial control systems (ICS) such as electrical power grids and water treatment plants, are prone to failure due to external attacks and internal mistakes or threats. Attacks and failures on safety-critical ICS have been prevalent in the past few decades and remain to be on the rise [1].

Steps are being taken to counter the increasing amount and sophistication of threats to CPS and ICS, which include automated surveillance and intrusion/anomaly detection systems (IDS). There is an abundance of works within CPS IDS research that focus on the systems-side of the overall interaction between humans and CPS [2], but few mentions of the human-side, which are often abstracted away. Human operator mistakes and insider threats have been at the core of some of the most significant CPS failures in recent history [3], so the human element directly involved in these systems needs to be more strongly considered in their design and implementation. We frame our work around the research question of "How can we model and simulate realistic human decision-making that directly impacts a cyber-physical system's operation and control processes?".

Contributions:

- We propose Cyber-Human Interaction Modeling for Cyber-Physical Systems (CHIMPS), a novel decision-making-based process for modeling human behavior meant for explicitly integrating high-fidelity human models into CPS/ICS state estimation models.
- We present a use case of our process, utilizing a human behavior-modeling framework [4] and a CPS real-time simulating framework [5] that serves as a proof-of-concept.

II. Process Overview

We propose a novel process, referred to as CHIMPS, that provides a starting point for the substantial work required to create a high-fidelity model and simulation of human behavior within CPS by first considering decision-making. We acknowledge and address the following current challenges in CPS research with our proposed process:

- There is a lack of research within CPS modeling that includes a human model or considers cases where a human operator is directly involved in maintaining the system control loop. Our process provides a way to directly include such a human model into CPS modeling with an added fresh perspective through cognitive science.
- With the expansiveness of human behavior, there is an overwhelmingly large state space to consider, with some examples being environmental conditions, emotions and intent, and interactions with other humans. We scope out a minor part of a more significant problem by offering initial approaches to modeling a single human operator's actions and decisions that directly affect system control processes and operation.
- Without providing a bound on the number of possible actions a human operator can perform, there is high potential complexity in system modeling if there is no focus on what kind of actions. We bound this complexity by focusing only on the core human-cyber interactions necessary for proper system operation.

CHIMPS breaks down into a four-step plan:

- Step 1: Scope and model only the human agent actions and behaviors directly impacting the CPS being analyzed.
- Step 2: Build or implement a CPS simulator matching your use case.
- Step 3: Combine the human actions agent model and the CPS simulator using a central communication software hub.
- Step 4: Set up the desired experiment and simulations and evaluate the decisions made.

We can use the resulting implementation from CHIMPS to study further research problems focused on why specific decision-making may result in certain human-made mistakes or insider threats. Depending on different preconditions of the CPS state or information provided to the human operator, we can attempt to trace where a system failure starts to form in the control loop and what decisions can prevent or escalate further issues.

III. Use Case and Implementation

We present our use case, focusing on a safety-critical ICS, that implements CHIMPS and simulates a human ICS operator directly interacting with a water treatment plant's control processes. Our use case revolves around a realistic scenario of a human ICS operator working in a water treatment plant, with the operator having the goals of maintaining the plant's regular operation and ensuring raw water properly gets treated for safe reuse. We use the following technologies in our implementation:

- **Deter Agents Simulating Humans (DASH)** - DASH is a dual-process cognitive architecture breaking decision-making into rational and instinctive behaviors that can be used to build human agent simulations [4]. We use DASH to model and simulate a human ICS operator.
- **MiniCPS** - MiniCPS is used to simulate network traffic and physical layer interaction in CPS [5]. We use a MiniCPS example implementation of the Secure Water Treatment (SWaT) testbed to mimic the physical processes of a real water treatment operation as the CPS simulator.
- **PyZMQ** - We use PyZMQ, a Python version of an open-source universal messaging library known as ZeroMQ [6], to create the central communication hub.

With these components working together, we can simulate a human ICS operator maintaining a water treatment plant's storage in a tank, intake, and outtake of raw water. Figure 1 demonstrates how the three components interact with one another.

Replication: To view the code of our implementation and further details on how to replicate it, you can access it at https://github.com/StengoS/CPSOperatorSim.

IV. Discussion and Future Work

We now look towards designing an experiment that takes a more in-depth look at the complex decisions where a human operator may consider multiple reasonable actions depending on the given system state. The next immediate steps are to extend our use case to involve more physical processes of SWaT and add more corresponding actions to our DASH ICS operator. There is also currently no explicit step to ensure the validity of the decisions being made from the human actions agent model, which is an ongoing area in extending our use case.

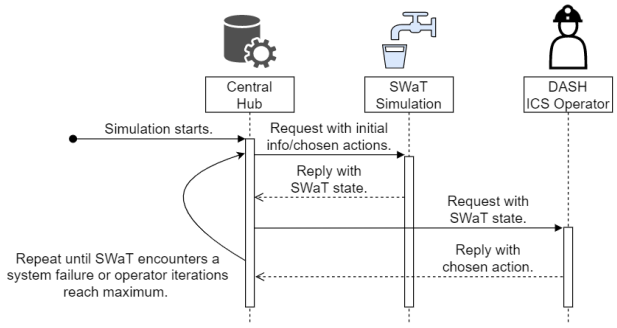

Fig. 1. Sequence diagram of how the DASH ICS operator-water treatment testbed simulation works

Future work will shift towards applying CHIMPS to modeling other kinds of CPS/ICS, including unmanned aerial vehicles, and refining it towards creating high-fidelity human cognitive models. We are interested in how we can design and automatically develop formal definitions of CPS that include human-cyber interactions using CHIMPS, specifically by incorporating the decision-making process and resulting system state into the formal specification for creating a behavior-specification-based IDS that accounts for human mistakes and insider threats. We also would like to evaluate the usability of CHIMPS and how researchers and CPS engineers can best use it to model new and existing systems, especially in an interdisciplinary context.

Acknowledgements

This research was done through the University of Southern California, Information Sciences Institute's Research Experience for Undergraduate (REU) Site "SURF-I: Safe, Usable, Reliable and Fair Internet". We thank the National Science Foundation for supporting the REU through NSF grant award #2051101.

References

[1] A. Ginter, "The Top 20 Cyberattacks on Industrial Control Systems," Tech. Rep., May 2018.
[2] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," vol. 46, no. 4, mar 2014. [Online]. Available: https://doi.org/10.1145/2542049
[3] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, and B. Green, "Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems," *International Journal of Critical Infrastructure Protection*, vol. 35, p. 100464, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1874548221000524
[4] J. Blythe, "A dual-process cognitive model for testing resilient control systems," in *2012 5th International Symposium on Resilient Control Systems*, 2012, pp. 8–12.
[5] "MiniCPS," https://github.com/scy-phy/minicps.
[6] "ZeroMQ," https://zeromq.org/.