A Formal Verification and Implementation Stack for Programmable Logic Controllers

Challenge:

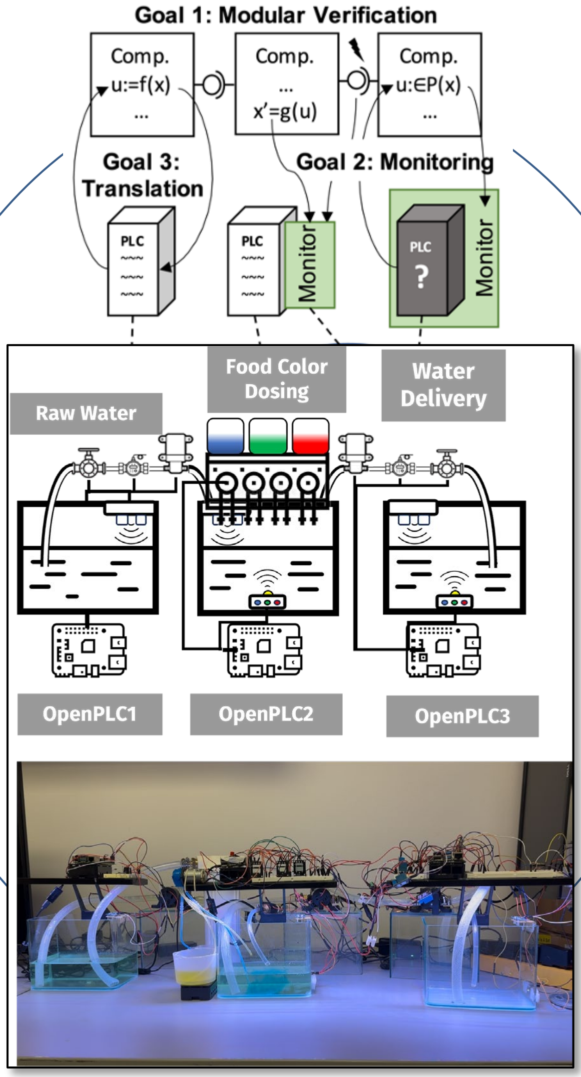
- **Modular verification:** multi-task PLC models, hardware malfunction and security attacks
- **Runtime monitoring:** trace violations, monitor legacy components
- **Translation:** compile formal models to PLC code

Solution:

- **Formalization of PLC components** and physical/industrial processes
- **Attack formalization** $[(\text{attack}^d ; \text{ctrl} ; \text{plant})^*]\text{safe}$
- **Industrial/community testbeds**
- Proof-guided **monitor synthesis**
- Code by **refinement proofs**

Luis Garcia, University of Utah (la.garcia@utah.edu)
Stefan Mitsch, DePaul University (smitsch@depaul.edu)

NSF CCF 2427581



Scientific Impact:

- Logic for compositional proofs of **communicating hybrid programs**
- **Refinement proofs** to turn nondeterministic system and threat models into deterministic control and detection code
- Verified **numerical approximations** and **quantifier elimination**

Broader Impact and Broader Participation:

- Ensure safety and reliability of critical infrastructure, e.g., water treatment plants
- TTP: Tools for engineers to design resilient industrial systems
- Education modules (e.g., miniSWAT, CPS courses), and industry collaboration

The NSF Formal Methods in the Field PI Meeting (2024 FMitF PI Meeting)
November 12-13, 2024 | The University of Iowa | Iowa City, Iowa