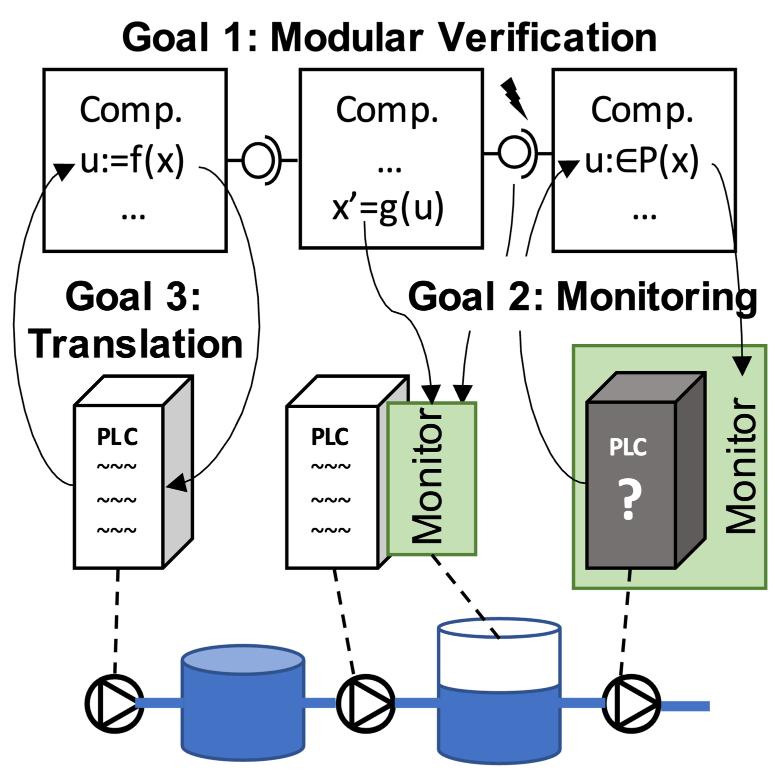
Collaborative Research: FMitF: Track I: A Formal Verification and Implementation Stack for Programmable Logic Controllers

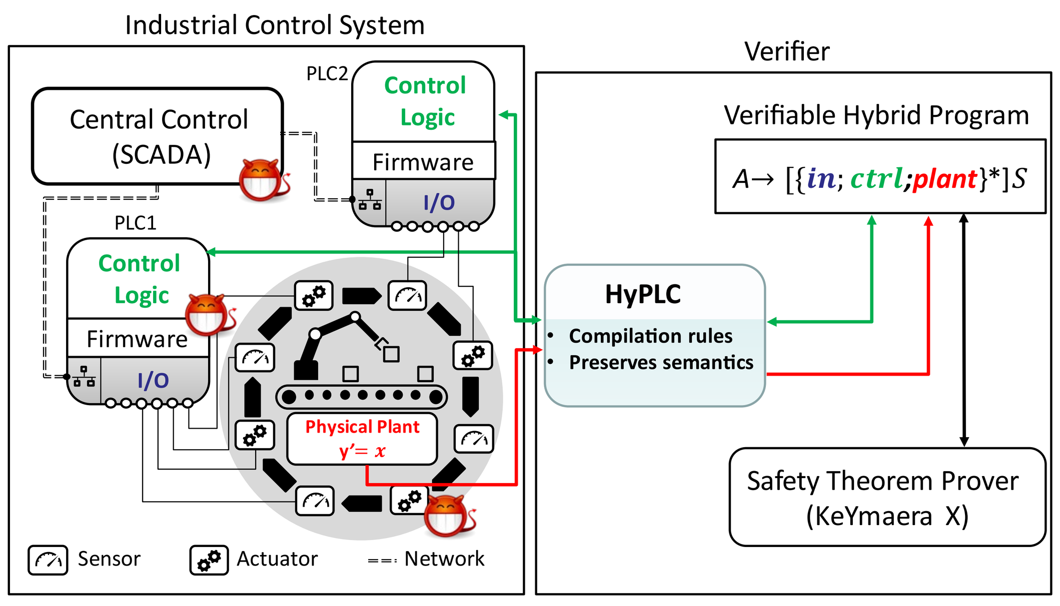
PIs: Stefan Mitsch (DePaul University), Luis Garcia (University of Utah)

Overview



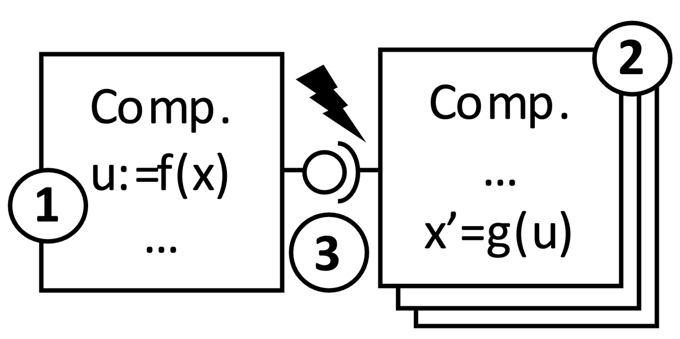
- **Modular verification**: multi-task PLC models, hardware malfunction and security attack models
- **Runtime monitoring**: trace violations, monitor legacy components
- **Bidirectional translation**: compile nondeterministic models to deterministic code

Challenges



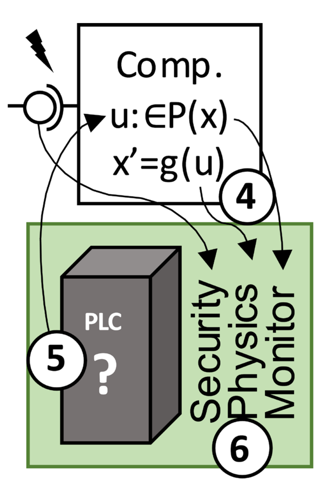
Approach

Component-based Formal Modeling and Verification



- Communication between components
- Formalize multi-task models

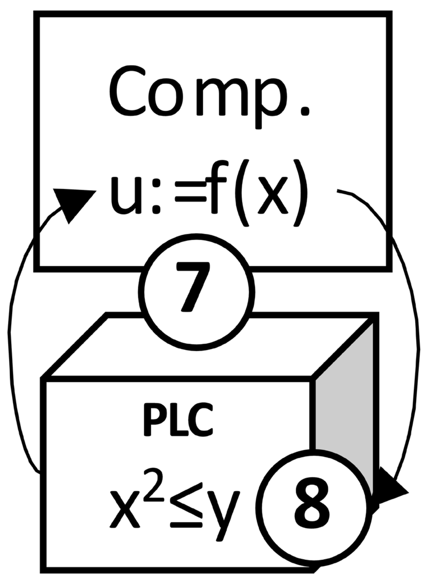
Verified Runtime Monitoring



- ModelPlex monitors to safeguard legacy components
- Unobservable true state

Verified Bidirectional Translation between Models and PLC Code

- Create a compilation chain from nondeterministic formal models to deterministic control and monitor code through refinement proofs



Key Innovations

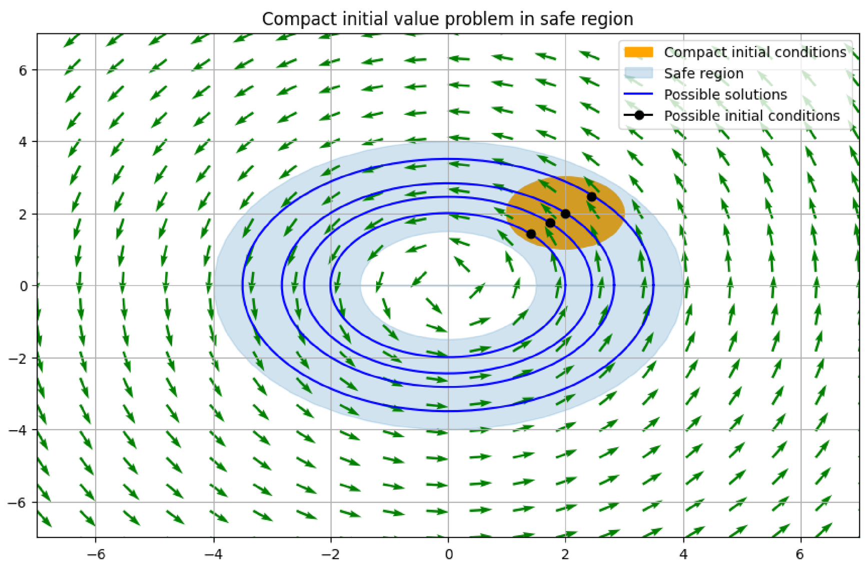
- **Formal models** of attack signatures and attack mitigation:

  [attack]<ctrl>safe

- Formalization of **PLC scan cycle**
- **Refinement proofs** to generate deterministic control code from nondeterministic models

Scientific Impact

- Provably correct **numerical approximations**
- Logic dL_{CHP} for **compositional proofs of communicating hybrid programs**



Broader Impact

Societal Importance: Ensures the safety and reliability of critical infrastructure like water treatment plants, nuclear reactors, and power grids, reducing risks related to malfunctions and cyberattacks.

Dependability: Provides tools that can be used by engineers in designing more resilient industrial systems.

Educational Modules: The methods and tools developed (e.g., KeYmaera X) will be integrated into existing undergraduate and graduate courses on cyber-physical systems.

Outreach: Collaboration with industry partners (e.g., Siemens) and dissemination of tools for educational and professional use.

Workforce Development: Through educational outreach and partnerships, the project will enhance the skill sets of engineers working with ICS.

Broader Dissemination: The tools and methodologies will be shared via open-source platforms, ensuring widespread access to the project's outcomes.