Formal Synthesis of Hybrid Controllers for Nuclear Power

PI: Dane Sabo, NRC Fellow, University of Pittsburgh
Friday 10th October, 2025

The goal of this research is to develop a methodology for creating autonomous hybrid control systems with guarantees of safe and correct behavior.

Nuclear power plants require the highest levels of control system reliability, where failures can result in significant economic losses, service interruptions, or radiological release. Currently, nuclear power relies on extensively trained operators who follow detailed written procedures to manage reactor control. These operators make critical decisions about when to switch between control objectives based on their interpretation of plant conditions and procedural guidance. However, this reliance on human operators prevents autonomous control and creates an economic challenge for next-generation nuclear power plants. Small modular reactors face significantly higher per-megawatt staffing costs than conventional plants, threatening their economic viability. Autonomous control systems are needed that can safely manage complex operational sequences with the same assurance as human-operated systems, but without constant supervision.

To address this need, we will combine formal methods with control theory to build hybrid control systems that are correct by construction. Hybrid systems use discrete logic to switch between continuous dynamic modes, similar to how operators change control strategies. Existing formal methods can generate provably correct switching logic with reactive synthesis, but cannot incorporate continuous dynamics or hybrid system transitions. Traditional control theory verifies continuous behavior but lacks tools for proving discrete switching correctness. We will combine tools from these two fields to build autonomous hybrid control systems that are correct by construction. We will formalize existing procedures into logical specifications and verify that continuous dynamics satisfy transition requirements between discrete modes. This approach will enable autonomous control in nuclear power plants while maintaining required safety standards.

If this research is successful, we will be able to do the following:

1. **Synthesize written procedures into verified control logic.** We will develop a methodology for converting written operating procedures into formal specifications. These specifications can be automatically synthesized into discrete control logic using reactive synthesis tools. This process uses structured intermediate representations to bridge natural language and mathematical logic. Control engineers will be able to generate verified mode-switching controllers from regulatory procedures with little formal methods expertise, reducing barriers to high-assurance control systems.
2. **Verify continuous control behavior across mode transitions.** We will establish methods for analyzing continuous control modes to ensure they satisfy discrete transition requirements. Using classical control theory for linear systems and reachability analysis for nonlinear dynamics, we verify each continuous mode safely reaches intended transitions. Engineers will be able to design continuous controllers using standard practices while ensuring system correctness and proving mode transitions occur safely at the right times.
3. **Demonstrate autonomous reactor startup control with safety guarantees.** We will apply this methodology to develop an autonomous controller for nuclear reactor startup. We will implement this methodology on a small modular reactor simulation using industry-standard control hardware. This trial will include multiple coordinated control modes from cold shutdown through criticality to power operation. This will provide evidence that autonomous hybrid control can be realized with current equipment, establishing a path toward reducing operator staffing while maintaining safety.

The innovation is unifying discrete synthesis and continuous verification to enable end-to-end correctness guarantees for hybrid systems. If successful, control engineers will be able to create autonomous controllers from existing procedures with mathematical proof of correct behavior, making high-assurance autonomous control practical for safety-critical applications. This capability is essential for economic viability of next-generation nuclear power. Small modular reactors represent a promising solution to growing energy demands, but success depends on reducing per-megawatt operating costs through increased autonomy. This research will provide the tools to achieve that autonomy while maintaining the exceptional safety record required by the nuclear industry.