## Formal Synthesis of Hybrid Controllers for Nuclear Power

**PI: Dane Sabo, NRC Fellow, University of Pittsburgh**

The goal of this research is to develop a methodology for creating autonomous control systems with event-driven control laws that have guarantees of safe and correct behavior.

Nuclear power relies on extensively trained operators who follow detailed written procedures to manage reactor control. Based on these procedures and operators' interpretation of plant conditions, operators make critical decisions about when to switch between control objectives. While human operators have maintained the nuclear industry's exceptional safety record, reliance on human operators has created 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 from computer science with control theory to build hybrid control systems that are correct by construction. Hybrid systems use discrete logic to switch between continuous control modes, similar to how operators change control strategies. Existing formal methods generate provably correct switching logic but cannot handle continuous dynamics during transitions, while traditional control theory verifies continuous behavior but lacks tools for proving discrete switching correctness. We will bridge this gap through a three-stage methodology. First, we will translate written operating procedures into temporal logic specifications using NASA's Formal Requirements Elicitation Tool (FRET), which structures requirements into scope, condition, component, timing, and response elements. This structured approach enables realizability checking to identify conflicts and ambiguities in procedures before implementation. Second, we will synthesize discrete mode switching logic from these specifications using reactive synthesis tools such as Strix, which generates deterministic automata that are provably correct by construction. Third, we will develop and verify continuous controllers for each discrete mode using standard control theory and reachability analysis. We will classify continuous modes based on their transition objectives, and then employ assume-guarantee contracts and barrier certificates to prove that mode transitions occur safely and as defined by the deterministic automata. This compositional approach enables local verification of continuous modes without requiring global trajectory analysis across the entire hybrid system. We will demonstrate this methodology by developing an autonomous startup controller for a Small Modular Advanced High Temperature Reactor (SmAHTR) and implementing it on an Emerson Ovation control system using the ARCADE hardware-in-the-loop platform. This approach will demonstrate autonomous control can be used for complex nuclear power operations while maintaining safety guarantees.

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 will be 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 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 develop methods using reachability analysis to ensure continuous control modes satisfy discrete transition requirements. 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 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 on a SmAHTR reactor simulation in a hardware-in-the-loop experiment. Control engineers will be able to implement high-assurance autonomous controls on industrial platforms they already use, enabling users to achieve autonomy without retraining costs or developing new equipment.