From Cold Start to Critical: Formal Synthesis of Hybrid Controllers

PI: Dane A. Sabo
dane.sabo@pitt.edu

Advisor: Dr. Daniel G. Cole
dgcole@pitt.edu

Wednesday 3rd September, 2025

1 Goals and Outcomes

The goal of this research is to use formal methods to create high-assurance hybrid control systems. Hybrid control systems have great potential for implementation in autonomous control as they are able to change control laws based on discrete triggers in the operating range of the controller. This allows the autonomous controller to use several easily tractable control laws for different regions in the state space, instead of using one controller over the entire systems operating range. But, the discrete jumps between control laws in a hybrid controller present challenges in proving stability and liveness properties of the whole system. While tools from control theory can prove properites for each individual control mode, they do not generalize when switching between control laws is introduced.

This research will take a different approach to hybrid controller synthesis and verification. Using tools from the formal methods community, we will create controllers that are correct-by-construction and allow guarantees to be made about the whole system's behavior. To demonstrate this, an autonomous controller for a nuclear power plant startup procedure will be created. Nuclear power is an excellent test case for this work as the continous piece of reactor dynamics is well studied, while the discrete component of mode switching is explicitly stated in regulatory requirements and operating procedures. Nuclear reactor control today *is* a hybrid control system–many functions in the control room use automated controllers for basic tasks, but the engagement and selection of these controllers is done by human operators referencing procedures to make decisions.

The capability to create high-assurance hybrid control systems has the potential to reduce the labor required to operate critical systems by removing the human operator from the loop. Nuclear power stands to greatly benefit from greater controller autonomy as the largest expense for reactors today is operations and maintenance. Technologies such as microreactors and modular reactors will improve the maintenance costs required through the use of factory-made replacement components, but will suffer increased operating costs per megawatt produced if they are required to staff the same way reactors today are staffed. But, if increased autonomy can be introduced, these costs will be ameliorated.

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

1. **Formalize mode switching requirements as logical specifications that can be translated into discrete controller implementations.**
2. **Categorize different continuous controller modes by their strategic relavance.** Different control modes serve one of two purposes: they may be transitory or stabilizing. Knowing when to switch from one control mode to another is handled by the discrete component of the hybrid system, but this outcome will identify the properties the continous components must satisfy for each controller mode.
3. **Verify that continuous controller modes satisfy dynamic requirements.** For the discrete transitions between control modes to be useful, we must ensure that the continous control modes will actually move the system to the transition, or if stabilizing, keep the system from leaving the control mode.
4. **Prove that a hybrid system implementation achieve strategic goals across the entire controller operating range.** By creating discrete controller transitions from logical specifications that are correct-by-construction and validating that continous

components perform appropriately between discrete transitions, we can be confident that the hybrid system is free from defect and can be utilized as a critical autonomous controller.