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

Tuesday 2nd September, 2025

1 Goals and Outcomes

The goal of this research is to use formal methods to create control systems that can switch between operating modes with a high assurance of correct construction. Modern control systems today often exist as hybrid control systems. Hybrid systems are those that have both continuous and discrete dynamics. Because of this, hybrid systems cannot be fully analyzed using only tools from continuous or discrete methods. Today, hybrid control systems are unable to be completely verified, that is to say we do not currently have ways of being building hybrid control systems that we can be certain meet high level strategic objectives, or who's behavior is totally understood.

The ambiguity on hybrid system behavior is problematic when one of the most useful cases of hybrid system control is for improved autonomy of critical systems. Nuclear power is a salient example. For a nuclear reactor during start-up, every mode of power from initially cold-start, to controlled core heating, and eventually full operating power is well understood dynamically. For each of these modes, significant portions of the control are optimized using automated controllers for each stage. The problem that remains for human operators is choosing when to switch from control law to the next, and ensuring that the proper conditions are met to do so–but these conditions are also clearly defined in regulation and operating procedures a priori.

We can use the fact that these transition points are well understood in combination with formal methods to synthesize the discrete part of a hybrid system. From that point, we can have a robust chain of proof that our discrete jumps will happen only at the correct times. Once that is established, we can use reachability analysis and traditional control theory to ensure that each operation 'mode' satisfies liveness, stability, or performance requirements. With the combination of these two methods, we can be sure of correct behavior switching between modes, and that strategic goals remain met while transitioning from one mode switch to the next.

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

1. **Formalize** mode switching requirements as logical statements that can then be translated into a controller implementation. This piece will address the correct-by-construction generation of the mode switching controller.
2. **Categorize** different continuous modes by their strategic relevance. Certain modes exist as control laws from one mode to the next, such as a controlled heating rate on reactor start-up before reaching operational conditions. Other modes exist as stable regions, such as full-power operation.
3. **Verify** continuous modes and accompanying continuous control laws satisfy strategic requirements. This can be done with reachability analysis, and ensuring that each mode transition as allowed from the requirements synthesis squares up against the reachability analysis and the continuous dynamics.
4. **Prove** that a given hybrid system achieves strategic goals across hybrid control modes. By seperately formalizing and analyzing continuous dyanmics and discrete dynamics, we can come back to say the whole hybrid system has met a strong guarantee of requirement adherence.