High-Assurance Hybrid Controller Synthesis from Logical Specifications

PI: Dane A. Sabo, dane.sabo@pitt.edu
Advisor: Daniel G. Cole, dgcole@pitt.edu

Goal: The goal of this research is to use mathematical statements of requirements and automated tools to construct hybrid controllers that are provably free from design defects.

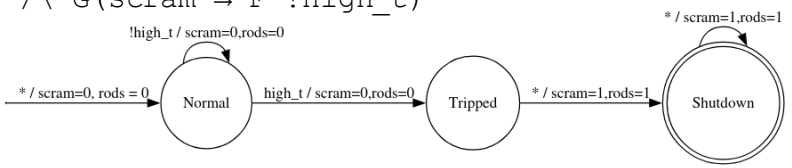
Outcomes: If this research is successful, we should be able to do the following:

1. Formalize design requirements and operational conditions as temporal logic specifications
2. Determine whether a controller implementation can be realized from a set of specifications
3. For unrealizable systems, identify where specification refinement is necessary
4. For realizable systems, synthesize the formal specification into a controller implementation

Controller Synthesis

- During normal operation, if a high temperature alarm is triggered, the reactor will immediately shutdown by inserting the control rods
- Once shutdown, the reactor will be unable to restart

```
G(high_t → X scram)
/\ G(scram → G rods)
/\ G(scram → (!scram U high_t))
/\ G(scram → F !high_t)
```



This research converts high-level requirements into logical specifications and uses automated tools to synthesize controller implementations.

Approach: Nuclear reactors are well studied systems of which we identify critical requirements during design. These requirements will be formalized as logical specifications. The core challenge of this research will be **automatically synthesizing** these specifications into a controller implementation that is **provably free of defects**. This process will include establishing whether a set of requirements are realizable. Realizable controllers in this context are derived from a set of specifications that provide sufficient detail to create an actual controller implementation. If a controller is not realizable, specification refinement guidance will be provided. Freedom from defects will be ensured by the use of automated formal methods tools.

Impact: Operations and maintenance are the largest costs in nuclear power. Conventional reactors are custom-built and require large maintenance teams, but relatively few operators. Small modular reactors (SMRs) and microreactors (MRs) invert this model: factory-made modules reduce construction and maintenance costs, but operator wages will become a major expense. If staffing needs stay the same, SMRs and MRs face stiff economic headwinds compared to other sources of power generation. By developing autonomous controllers with strong safety and performance guarantees, we can reduce operator burden, lower staffing requirements, and improve the economic viability of SMRs and MRs.