From Cold Start to Critical:
Formal Synthesis of Autonomous Hybrid Controllers

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

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

Track: PhD Mechanical Engineering

Friday 5th December, 2025

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. But, 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. 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 using reactive synthesis to generate deterministic automata that are provably correct by construction. Third, we will develop 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 on an Emerson Ovation control system. 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. 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. 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.

Contents

1 Goals and Outcomes

The goal of this research is to develop a methodology for creating autonomous hybrid control systems with mathematical 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 plant operations rely on extensively trained human operators who follow detailed written procedures and strict regulatory requirements to manage reactor control. These operators make critical decisions about when to switch between different control modes based on their interpretation of plant conditions and procedural guidance. This reliance on human operators prevents autonomous control capabilities and creates a fundamental economic challenge for next-generation reactor designs. Small modular reactors, in particular, face per-megawatt staffing costs far exceeding those of conventional plants and threaten their economic viability.

What is needed is a method to create autonomous control systems that safely manage complex operational sequences with the same assurance as human-operated systems, but without constant human 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 control modes, mirroring how operators change control strategies. Existing formal methods can generate provably correct switching logic from written requirements, but they cannot handle the continuous dynamics that occur during transitions between modes. Meanwhile, traditional control theory can verify continuous behavior but lacks tools for proving correctness of discrete switching decisions. By synthesizing discrete mode transitions directly from written operating procedures and verifying continuous behavior between transitions, we can create hybrid control systems with end-to-end correctness guarantees. If existing procedures can be formalized into logical specifications and continuous dynamics verified against transition requirements, then autonomous controllers can be built that are provably free from design defects. This approach will enable autonomous control in nuclear power plants while maintaining the high safety standards required by the industry.

This work is conducted within the University of Pittsburgh Cyber Energy Center, which provides access to industry collaboration and Emerson control hardware, ensuring that developed solutions align with practical implementation requirements.

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

1. **Translate written procedures into verified control logic.** We will develop a methodology for converting existing written operating procedures into formal specifications that can be automatically synthesized into discrete control logic. This process will use structured intermediate representations to bridge natural language procedures and mathematical logic. Control system engineers will generate verified mode-switching controllers directly from regulatory procedures without formal methods expertise, lowering the barrier 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 will verify that each continuous mode safely reaches its intended transitions. Engineers will design continuous controllers using standard practices while iterating

to ensure broader system correctness, proving that mode transitions occur safely and at the correct times.

3. **Demonstrate autonomous reactor startup control with safety guarantees.** We will apply this methodology to develop an autonomous controller for nuclear reactor startup procedures, implementing it on a small modular reactor simulation using industry-standard control hardware. This demonstration will prove correctness across multiple coordinated control modes from cold shutdown through criticality to power operation. We will demonstrate that autonomous hybrid control can be realized in the nuclear industry with current equipment, establishing a path toward reduced operator staffing while maintaining safety.

The innovation in this work is unifying discrete synthesis with continuous verification to enable end-to-end correctness guarantees for hybrid systems. If successful, control engineers will create autonomous controllers from existing procedures with mathematical proof of correct behavior. High-assurance autonomous control will become practical for safety-critical applications. This capability is essential for the economic viability of next-generation nuclear power. Small modular reactors offer a promising solution to growing energy demands, but their 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 the nuclear industry requires.

2 State of the Art and Limits of Current Practice

The principal aim of this research is to create autonomous reactor control systems that are tractably safe. To understand what is being automated, we must first understand how nuclear reactors are operated today. This section examines reactor operators and the operating procedures we aim to leverage, then investigates limitations of human-based operation, and concludes with current formal methods approaches to reactor control systems.

2.1 Current Reactor Procedures and Operation

Nuclear plant procedures exist in a hierarchy: normal operating procedures for routine operations, abnormal operating procedures for off-normal conditions, Emergency Operating Procedures (EOPs) for design-basis accidents, Severe Accident Management Guidelines (SAMGs) for beyond-design-basis events, and Extensive Damage Mitigation Guidelines (EDMGs) for catastrophic damage scenarios. These procedures must comply with 10 CFR 50.34(b)(6)(ii) and are developed using guidance from NUREG-0900 [1, 2], but their development relies fundamentally on expert judgment and simulator validation rather than formal verification. Procedures undergo technical evaluation, simulator validation testing, and biennial review as part of operator requalification under 10 CFR 55.59 [3]. Despite this rigor, procedures fundamentally lack formal verification of key safety properties. No mathematical proof exists that procedures cover all possible plant states, that required actions can be completed within available timeframes, or that transitions between procedure sets maintain safety invariants.

LIMITATION: *Procedures lack formal verification of correctness and completeness.* Current procedure development relies on expert judgment and simulator validation. No mathematical proof exists that procedures cover all possible plant states, that required actions can be completed within available timeframes, or that transitions between procedure sets maintain safety invariants. Paper-based procedures cannot ensure correct application, and even computer-based procedure systems lack the formal guarantees that automated reasoning could provide.

Nuclear plants operate with multiple control modes: automatic control, where the reactor control system maintains target parameters through continuous reactivity adjustment; manual control, where operators directly manipulate the reactor; and various intermediate modes. In typical pressurized water reactor operation, the reactor control system automatically maintains a floating average temperature and compensates for power demand changes through reactivity feedback loops alone. Safety systems, by contrast, operate with implemented automation. Reactor Protection Systems trip automatically on safety signals with millisecond response times, and engineered safety features actuate automatically on accident signals without operator action required.

The division between automated and human-controlled functions reveals the fundamental challenge of hybrid control. Highly automated systems handle reactor protection—automatic trips on safety parameters, emergency core cooling actuation, containment isolation, and basic process control [4, 5]. Human operators, however, retain control of strategic decision-making: power level changes, startup/shutdown sequences, mode transitions, and procedure implementation.

2.2 Human Factors in Nuclear Accidents

Current-generation nuclear power plants employ over 3,600 active NRC-licensed reactor operators in the United States [6]. These operators divide into Reactor Operators (ROs), who manipulate reactor controls, and Senior Reactor Operators (SROs), who direct plant operations and serve as shift supervisors [7]. Staffing typically requires at least two ROs and one SRO for current-generation units [8]. Becoming a reactor operator requires several years of training.

The persistent role of human error in nuclear safety incidents—despite decades of improvements in training and procedures—provides the most compelling motivation for formal automated control with mathematical safety guarantees. Operators hold legal authority under 10 CFR Part 55 to make critical decisions, including departing from normal regulations during emergencies. The Three Mile Island (TMI) accident demonstrated how a combination of personnel error, design deficiencies, and component failures led to partial meltdown when operators misread confusing and contradictory readings and shut off the emergency water system [9]. The President's Commission on TMI identified a fundamental ambiguity: placing responsibility for safe power plant operations on the licensee without formal verification that operators can fulfill this responsibility does not guarantee safety. This tension between operational flexibility and safety assurance remains unresolved: the person responsible for reactor safety is often the root cause of failures.

Multiple independent analyses converge on a striking statistic: 70–80% of nuclear power plant events are attributed to human error, versus approximately 20% to equipment failures [10]. More significantly, the root cause of all severe accidents at nuclear power plants—Three Mile Island, Chernobyl, and Fukushima Daiichi—has been identified as poor safety management and safety culture: primarily human factors [11]. A detailed analysis of 190 events at Chinese nuclear power plants from 2007–2020 [12] found that 53% of events involved active errors, while 92% were associated with latent errors—organizational and systemic weaknesses that create conditions for failure.

LIMITATION: *Human factors impose fundamental reliability limits that cannot be overcome through training alone.* The persistent human error contribution despite four decades of improvements demonstrates that these limitations are fundamental rather than a remediable part of human-driven control.

2.3 HARDENS and Formal Methods

The High Assurance Rigorous Digital Engineering for Nuclear Safety (HARDENS) project represents the most advanced application of formal methods to nuclear reactor control systems to date [13].

HARDENS aimed to address a fundamental dilemma: existing U.S. nuclear control rooms rely on analog technologies from the 1950s–60s. This technology is obsolete compared to modern control systems and incurs significant risk and cost. The NRC contracted Galois, a formal methods firm, to demonstrate that Model-Based Systems Engineering and formal methods could design, verify, and implement a complex protection system meeting regulatory criteria at a fraction of typical cost. The project delivered a Reactor Trip System (RTS) implementation with full traceability from NRC Request for Proposals and IEEE standards through formal architecture specifications to verified software.

HARDENS employed formal methods tools and techniques across the verification hierarchy. High-level specifications used Lando, SysMLv2, and FRET (NASA Formal Requirements Elicitation Tool) to capture stakeholder requirements, domain engineering, certification requirements, and safety requirements. Requirements were analyzed for consistency, completeness, and realizability using SAT and SMT solvers. Executable formal models used Cryptol to create a behavioral model of the entire RTS, including all subsystems, components, and limited digital twin models of sensors, actuators, and compute infrastructure. Automatic code synthesis generated verifiable C implementations and SystemVerilog hardware implementations directly from Cryptol models—eliminating the traditional gap between specification and implementation where errors commonly arise.

Despite its accomplishments, HARDENS has a fundamental limitation directly relevant to hybrid control synthesis: the project addressed only discrete digital control logic without modeling or verifying continuous reactor dynamics. The Reactor Trip System specification and verification covered discrete state transitions (trip/no-trip decisions), digital sensor input processing through discrete logic, and discrete actuation outputs (reactor trip commands). The project did not address continuous dynamics of nuclear reactor physics. Real reactor safety depends on the interaction between continuous processes—temperature, pressure, neutron flux—evolving in response to discrete control decisions. HARDENS verified the discrete controller in isolation but not the closed-loop hybrid system behavior.

LIMITATION: *HARDENS addressed discrete control logic without continuous dynamics or hybrid system verification.* Verifying discrete control logic alone provides no guarantee that the closed-loop system exhibits desired continuous behavior such as stability, convergence to setpoints, or maintained safety margins.

HARDENS produced a demonstrator system at Technology Readiness Level 2–3 (analytical proof of concept with laboratory breadboard validation) rather than a deployment-ready system validated through extended operational testing. The NRC Final Report explicitly notes [13] that all material is considered in development, not a finalized product, and that "The demonstration of its technical soundness was to be at a level consistent with satisfaction of the current regulatory criteria, although with no explicit demonstration of how regulatory requirements are met." The project did not include deployment in actual nuclear facilities, testing with real reactor systems under operational conditions, side-by-side validation with operational analog RTS systems, systematic failure mode testing (radiation effects, electromagnetic interference, temperature extremes), NRC licensing review, or human factors validation with licensed operators in realistic control room scenarios.

LIMITATION: *HARDENS achieved TRL 2–3 without experimental validation.* While formal verification provides mathematical correctness guarantees for the implemented discrete logic, the gap between formal verification and actual system deployment involves myriad practical considerations: integration with legacy systems, long-term reliability under harsh environments, human-system interaction in realistic operational contexts, and regulatory acceptance of formal methods as primary assurance evidence.

3 Research Approach

This research will overcome the limitations of current practice to build high-assurance hybrid control systems for critical infrastructure. Building these systems with formal correctness guarantees requires three main thrusts:

1. Translate operating procedures and requirements into temporal logic formulae
2. Create the discrete half of a hybrid controller using reactive synthesis
3. Develop continuous controllers to operate between modes, and verify their correctness

Commercial nuclear power operations remain manually controlled by human operators, yet the procedures they follow are highly prescriptive and well-documented. This suggests that human operators may not be entirely necessary given current technology. Written procedures and requirements are sufficiently detailed that they may be translatable into logical formulae with minimal effort. If successful, this approach enables automation of existing procedures without system reengineering. To formalize these procedures, we will use temporal logic, which captures system behaviors through temporal relations.

The most efficient path for this translation is NASA's Formal Requirements Elicitation Tool (FRET). FRET employs a specialized requirements language called FRETish that restricts requirements to easily understood components while eliminating ambiguity [14]. FRETish bridges natural language and mathematical specifications through a structured English-like syntax automatically translatable to temporal logic.

FRET enforces this structure by requiring all requirements to contain six components:

1. Scope: *What modes does this requirement apply to?*
2. Condition: *Scope plus additional specificity*
3. Component: *What system element does this requirement affect?*
4. Shall
5. Timing: *When does the response occur?*
6. Response: *What action should be taken?*

FRET provides functionality to check system *realizability*. Realizability analysis determines whether written requirements are complete by examining the six structural components. Complete requirements neither conflict with one another nor leave any behavior undefined. Systems that are not realizable from their procedure definitions and design requirements present problems beyond autonomous control implementation. Such systems contain behavioral inconsistencies—the physical equivalent of software bugs. Using FRET during autonomous controller development allows systematic identification and resolution of these errors.

The second category of realizability issues involves undefined behaviors typically left to human judgment during operations. This ambiguity is undesirable for high-assurance systems, since even well-trained humans remain prone to errors. Addressing these specification gaps in FRET during development yields controllers free from these vulnerabilities.

FRET exports requirements in temporal logic format compatible with reactive synthesis tools. Linear Temporal Logic (LTL) builds upon modal logic's foundational operators for necessity ($\square$, "box") and possibility ($\lozenge$, "diamond"), extending them to reason about temporal behavior [15]. The box operator $\square$ expresses that a property holds at all future times (necessarily always), while the diamond operator $\lozenge$ expresses that a property holds at some future time (possibly eventually). These are complemented by the next operator (X) for the immediate successor state and the until operator (U) for expressing persistence conditions.

Consider a nuclear reactor SCRAM requirement expressed in natural language: *"If a high temperature alarm triggers, control rods must immediately insert and remain inserted until operator reset."* This plain language requirement can be translated into a rigorous logical specification:

$$\square(HighTemp \rightarrow X(RodsInserted \wedge (\neg RodsWithdrawn\ U\ OperatorReset))) \tag{1}$$

This specification precisely captures the temporal relationship between the alarm condition, the required response, and the persistence requirement. The necessity operator $\square$ ensures this safety property holds throughout all possible future system executions, while the next operator X enforces immediate response. The until operator U maintains the state constraint until the reset condition occurs. No ambiguity exists in this scenario because all decisions are represented by discrete variables. Formulating operating rules in this logic enforces finite, correct operation.

Reactive synthesis is an active research field focused on generating discrete controllers from temporal logic specifications. The term "reactive" indicates that the system responds to environmental inputs to produce control outputs. These synthesized systems are finite, with each node representing a unique discrete state. The connections between nodes, called *state transitions*, specify the conditions under which the discrete controller moves from state to state. This complete mapping of possible states and transitions constitutes a *discrete automaton*. Discrete automata can be represented graphically as nodes (discrete states) with edges indicating transitions between them. From the automaton graph, one can fully describe discrete system dynamics and develop intuitive understanding of system behavior. Hybrid systems naturally exhibit discrete behavior amenable to formal analysis through these finite state representations.

We will employ state-of-the-art reactive synthesis tools, particularly Strix, which has demonstrated superior performance in the Reactive Synthesis Competition (SYNTCOMP) through efficient parity game solving algorithms [16, 17]. Strix translates linear temporal logic specifications into deterministic automata automatically while maximizing generated automata quality. Once constructed, the automaton can be implemented using standard programming control flow constructs. The graphical representation enables inspection and facilitates communication with controls programmers who lack formal methods expertise.

We will use discrete automata to represent the switching behavior of our hybrid system. This approach yields an important theoretical guarantee: because the discrete automaton is synthesized entirely through automated tools from design requirements and operating procedures, the automaton—and therefore our hybrid switching behavior—is *correct by construction*. Correctness of the switching controller is paramount. Mode switching represents the primary responsibility of human operators in control rooms today. Human operators possess the advantage of real-time judgment: when mistakes occur, they can correct them dynamically with capabilities extending beyond written procedures. Autonomous control lacks this adaptive advantage. Instead, autonomous controllers replacing human operators must not make switching errors between continuous modes. Synthesizing controllers from logical specifications with guaranteed correctness eliminates the possibility of switching errors.

While discrete system components will be synthesized with correctness guarantees, they represent only half of the complete system. Autonomous controllers like those we are developing exhibit continuous dynamics within discrete states. These systems, called hybrid systems, combine continuous dynamics (flows) with discrete transitions (jumps). These dynamics can be formally expressed as [18]:

$$\dot{x}(t) = f(x(t), q(t), u(t)) \tag{2}$$

$$q(k+1) = \nu(x(k), q(k), u(k)) \tag{3}$$

Here, $f(\cdot)$ defines the continuous dynamics while $\nu(\cdot)$ governs discrete transitions. The continuous states x, discrete state q, and control input u interact to produce hybrid behavior. The discrete state q defines which continuous dynamics mode is currently active. Our focus centers on continuous autonomous hybrid systems, where continuous states remain unchanged during jumps—a property naturally exhibited by physical systems. For example, a nuclear reactor switching from warm-up to load-following control cannot instantaneously change its temperature or control rod position, but can instantaneously change control laws.

The approach described for producing discrete automata yields physics-agnostic specifications representing only half of a complete hybrid autonomous controller. These automata alone cannot define the full behavior of the control systems we aim to construct. The continuous modes will be developed after discrete automaton construction, leveraging the automaton structure and transitions to design multiple smaller, specialized continuous controllers.

Notably, translation into linear temporal logic creates barriers between different control modes. Switching from one mode to another becomes a discrete boolean variable. $RodsInserted$ or $HighTemp$ in the temporal specifications are booleans, but in the real system they represent physical features in the state space. These features mark where continuous control modes end and begin; their definition is critical for determining which control mode is active at any given time. Information about where in the state space these conditions exist will be preserved from the original requirements and included in continuous control mode development, but will not appear as numeric values in discrete mode switching synthesis.

The discrete automaton transitions are key to the supervisory behavior of the autonomous controller. These transitions mark decision points for switching between continuous control modes and define their strategic objectives. We will classify three types of high-level continuous controller objectives based on discrete mode transitions:

1. **Stabilizing:** A stabilizing control mode has one primary objective: maintaining the hybrid system within its current discrete mode. This corresponds to steady-state normal operating modes, such as a full-power load-following controller in a nuclear power plant. Stabilizing modes can be identified from discrete automata as nodes with only incoming transitions.

2. **Transitory:** A transitory control mode has the primary goal of transitioning the hybrid system from one discrete state to another. In nuclear applications, this might represent a controlled warm-up procedure. Transitory modes ultimately drive the system toward a stabilizing steady-state mode. These modes may have secondary objectives within a discrete state, such as maintaining specific temperature ramp rates before reaching full-power operation.
3. **Expulsory:** An expulsory mode is a specialized transitory mode with additional safety constraints. Expulsory modes ensure the system is directed to a safe stabilizing mode during failure conditions. For example, if a transitory mode fails to achieve its intended transition, the expulsory mode activates to immediately and irreversibly guide the system toward a globally safe state. A reactor SCRAM exemplifies an expulsory continuous mode: when initiated, it must reliably terminate the nuclear reaction and direct the reactor toward stabilizing decay heat removal.

Building continuous modes after constructing discrete automata enables local controller design focused on satisfying discrete transitions. The primary challenge in hybrid system verification is ensuring global stability across transitions [18]. Current techniques struggle with this problem because dynamic discontinuities complicate verification [19,20]. This work alleviates these problems by designing continuous controllers specifically with transitions in mind. Decomposing continuous modes according to their required behavior at transition points avoids solving trajectories through the entire hybrid system. Instead, local behavior information at transition boundaries suffices. To ensure continuous modes satisfy their requirements, we employ three main techniques: reachability analysis, assume-guarantee contracts, and barrier certificates.

Reachability analysis computes the reachable set of states for a given input set. While trivial for linear continuous systems, recent advances have extended reachability to complex nonlinear systems [21,22]. We use reachability to define continuous state ranges at discrete transition boundaries and verify that requirements are satisfied within continuous modes. Assume-guarantee contracts apply when continuous state boundaries are not explicitly defined. For any given mode, the input range for reachability analysis is defined by the output ranges of discrete modes that transition to it. This compositional approach ensures each continuous controller is prepared for its possible input range, enabling reachability analysis without global system analysis. Finally, barrier certificates prove that mode transitions are satisfied. Barrier certificates ensure that continuous modes on either side of a transition behave appropriately by preventing system trajectories from crossing a given barrier. Control barrier functions certify safety by establishing differential inequality conditions that guarantee forward invariance of safe sets [23]. For example, a barrier certificate can guarantee that a transitory mode transferring control to a stabilizing mode will always move away from the transition boundary, rather than destabilizing the target stabilizing mode.

This compositional approach has several advantages. First, this approach breaks down autonomous controller design into smaller pieces. For designers of future autonomous control systems, the barrier to entry is low, and design milestones are clear due to the procedural nature of this research plan. Second, measurable design progress also enables measurement of regulatory adherence. Each step in this development procedure generates an artifact that can be independently evaluated as proof of safety and performance. Finally, the compositional nature of this development plan enables incremental refinement between control system layers. For example, difficulty developing a continuous mode may reflect a discrete automaton that is too restrictive, prompting refinement of system design requirements. This synthesis between levels promotes broader understanding of the autonomous controller.

To demonstrate this methodology, we will develop an autonomous startup controller for a Small Modular Advanced High Temperature Reactor (SmAHTR). We have already developed a high-fidelity SmAHTR model in Simulink that captures the thermal-hydraulic and neutron kinetics behavior essential for verifying continuous controller performance under realistic plant dynamics. The synthesized hybrid controller will be implemented on an Emerson Ovation control system platform, representative of industry-standard control hardware deployed in modern nuclear facilities. The Advanced Reactor Cyber Analysis and Development Environment (ARCADE) suite will serve as the integration layer, managing real-time communication between the Simulink simulation and the Ovation controller. This hardware-in-the-loop configuration enables validation of the controller implementation on actual industrial control equipment interfacing with a realistic reactor simulation, assessing computational performance, real-time execution constraints, and communication latency effects. Demonstrating autonomous startup control on this representative platform will establish both the theoretical validity and practical feasibility of the synthesis methodology for deployment in actual small modular reactor systems.

This unified approach addresses a fundamental gap in hybrid system design by bridging formal methods and control theory through a systematic, tool-supported methodology. Translating existing nuclear procedures into temporal logic, synthesizing provably correct discrete switching logic, and developing verified continuous controllers creates a complete framework for autonomous hybrid control with mathematical guarantees. The result is an autonomous controller that not only replicates human operator decision-making but does so with formal assurance that switching logic is correct by construction and continuous behavior satisfies safety requirements. This methodology transforms nuclear reactor control from a manually intensive operation requiring constant human oversight into a fully autonomous system with higher reliability than human-operated alternatives. More broadly, this approach establishes a replicable framework for developing high-assurance autonomous controllers in any domain where operating procedures are well-documented and safety is paramount.

4 Metrics for Success

This research will be measured by advancement through Technology Readiness Levels, progressing from fundamental concepts to validated prototype demonstration. This work begins at TRL 2–3 and aims to reach TRL 5, where system components operate successfully in a relevant laboratory environment. This section explains why TRL advancement provides the most appropriate success metric and defines the specific criteria required to achieve TRL 5.

Technology Readiness Levels provide the ideal success metric because they explicitly measure the gap between academic proof-of-concept and practical deployment—precisely what this work aims to bridge. Academic metrics like papers published or theorems proved cannot capture practical feasibility. Empirical metrics like simulation accuracy or computational speed cannot demonstrate theoretical rigor. TRLs measure both dimensions simultaneously. Advancing from TRL 3 to TRL 5 requires maintaining theoretical rigor while progressively demonstrating practical feasibility. Formal verification must remain valid as the system moves from individual components to integrated hardware testing.

The nuclear industry requires extremely high assurance before deploying new control technologies. Demonstrating theoretical correctness alone is insufficient for adoption; conversely, showing empirical performance without formal guarantees fails to meet regulatory requirements. TRLs capture this dual requirement naturally. Each level represents both increased practical maturity and sustained theoretical validity. Furthermore, TRL assessment forces explicit identification of remaining barriers to deployment. The nuclear industry already uses TRLs for technology assessment, making this metric directly relevant to potential adopters. Reaching TRL 5 provides a clear answer to industry questions about feasibility and maturity that academic publications alone cannot.

Moving from current state to target requires achieving three intermediate levels, each representing a distinct validation milestone:

TRL 3 ***Critical Function and Proof of Concept*** For this research, TRL 3 means demonstrating that each component of the methodology works in isolation. Startup procedures must be translated into temporal logic specifications that pass realizability analysis. A discrete automaton must be synthesized with interpretable structure. At least one continuous controller must be designed with reachability analysis proving transition requirements are satisfied. Independent review must confirm that specifications match intended procedural behavior. This proves the fundamental approach on a simplified startup sequence.

TRL 4 ***Laboratory Testing of Integrated Components*** For this research, TRL 4 means demonstrating a complete integrated hybrid controller in simulation. All startup procedures must be formalized with a synthesized automaton covering all operational modes. Continuous controllers must exist for all discrete modes. Verification must be complete for all mode transitions using reachability analysis, barrier certificates, and assume-guarantee contracts. The integrated controller must execute complete startup sequences in software simulation with zero safety violations across multiple consecutive runs. This proves that formal correctness guarantees can be maintained throughout system integration.

TRL 5 ***Laboratory Testing in Relevant Environment*** For this research, TRL 5 means demonstrating the verified controller on industrial control hardware through hardware-in-the-loop testing. The discrete automaton must be implemented on the Emerson Ovation control system and verified to match synthesized specifications exactly. Continuous controllers must execute at required rates. The ARCADE interface must establish stable real-time communication between the Emerson Ovation hardware and SmAHTR simulation. Complete autonomous startup sequences must execute via hardware-in-the-loop across the full operational envelope. The controller must handle off-nominal scenarios to validate that expulsory modes function correctly. For example, simulated sensor failures must trigger appropriate fault detection and mode transitions, and loss-of-cooling scenarios must activate SCRAM procedures as specified. Graded responses to minor disturbances are outside this work's scope. Formal verification results must remain valid, with discrete behavior matching specifications and continuous trajectories remaining within verified bounds. This proves that the methodology produces verified controllers implementable on industrial hardware.

Progress will be assessed quarterly through collection of specific data comparing actual results against TRL advancement criteria. Specification development status indicates progress toward TRL 3. Synthesis results and verification coverage indicate progress toward TRL 4. Simulation performance metrics and hardware integration milestones indicate progress toward TRL 5. The research plan will be revised only when new data invalidates fundamental assumptions. This research succeeds if it achieves TRL 5 by demonstrating a complete autonomous hybrid controller with formal correctness guarantees operating on industrial control hardware through hardware-in-the-loop testing in a relevant laboratory environment. This establishes both theoretical validity and practical feasibility, proving that the methodology produces verified controllers and that implementation is achievable with current technology.

5 Risks and Contingencies

This research relies on several critical assumptions that, if invalidated, would require scope adjustment or methodological revision. The primary risks to successful completion fall into four categories: computational tractability of synthesis and verification, complexity of the discrete-continuous interface, completeness of procedure formalization, and hardware-in-the-loop integration challenges. Each risk has associated indicators for early detection and contingency plans that preserve research value even if core assumptions prove false. The staged project structure ensures that partial success yields publishable results and clear identification of remaining barriers to deployment.

5.1 Computational Tractability of Synthesis

The first major assumption is that formalized startup procedures will yield automata small enough for efficient synthesis and verification. Reactive synthesis scales exponentially with specification complexity, creating risk that temporal logic specifications derived from complete startup procedures may produce automata with thousands of states. Such large automata would require synthesis times exceeding days or weeks, preventing demonstration of the complete methodology within project timelines. Reachability analysis for continuous modes with high-dimensional state spaces may similarly prove computationally intractable. Either barrier would constitute a fundamental obstacle to achieving the research objectives.

Several indicators would provide early warning of computational tractability problems. Synthesis times exceeding 24 hours for simplified procedure subsets would suggest complete procedures are intractable. Generated automata containing more than 1,000 discrete states would indicate the discrete state space is too large for efficient verification. Specifications flagged as unrealizable by FRET or Strix would reveal fundamental conflicts in the formalized procedures. Reachability analysis failing to converge within reasonable time bounds would show that continuous mode verification cannot be completed with available computational resources.

The contingency plan for computational intractability is to reduce scope to a minimal viable startup sequence. This reduced sequence would cover only cold shutdown to criticality to low-power hold, omitting power ascension and other operational phases. The subset would still demonstrate the complete methodology while reducing computational burden. The research contribution would remain valid even with reduced scope, proving that formal hybrid control synthesis is achievable for safety-critical nuclear applications. The limitation to simplified operational sequences would be explicitly documented as a constraint rather than a failure.

5.2 Discrete-Continuous Interface Formalization

The second critical assumption concerns the mapping between boolean guard conditions in temporal logic and continuous state boundaries required for mode transitions. This interface represents the fundamental challenge of hybrid systems: relating discrete switching logic to continuous dynamics. Temporal logic operates on boolean predicates, while continuous control requires reasoning about differential equations and reachable sets. Guard conditions requiring complex nonlinear predicates may resist boolean abstraction, making synthesis intractable. Continuous safety regions that cannot be expressed as conjunctions of verifiable constraints would similarly create insurmountable verification challenges. The risk extends beyond static interface definition to dynamic behavior across transitions: barrier certificates may fail to exist for proposed transitions, or continuous modes may be unable to guarantee convergence to discrete transition boundaries.

Early indicators of interface formalization problems would appear during both synthesis and verification phases. Guard conditions requiring complex nonlinear predicates that resist boolean abstraction would suggest fundamental misalignment between discrete specifications and continuous realities. Continuous safety regions that cannot be expressed as conjunctions of half-spaces or polynomial inequalities would indicate the interface between discrete guards and continuous invariants is too complex. Failure to construct barrier certificates proving safety across mode transitions would reveal that continuous dynamics cannot be formally related to discrete switching logic. Reachability analysis showing that continuous modes cannot reach intended transition boundaries from all possible initial conditions would demonstrate the synthesized discrete controller is incompatible with achievable continuous behavior.

The primary contingency for interface complexity is restricting continuous modes to operate within polytopic invariants. Polytopes are state regions defined as intersections of linear half-spaces, which map directly to boolean predicates through linear inequality checks. This restriction ensures tractable synthesis while maintaining theoretical rigor, though at the cost of limiting expressiveness compared to arbitrary nonlinear regions. The discrete-continuous interface remains well-defined and verifiable with polytopic restrictions, providing a clear fallback position that preserves the core methodology. Conservative over-approximations offer an alternative approach: a nonlinear safe region can be inner-approximated by a polytope, sacrificing operational flexibility to maintain formal guarantees. The three-mode classification already structures the problem to minimize complex transitions, with critical safety properties concentrated in expulsory modes that can receive additional design attention.

Mitigation strategies focus on designing continuous controllers with discrete transitions as primary objectives from the outset. Rather than designing continuous control laws independently and verifying transitions post-hoc, the approach uses transition requirements as design constraints. Control barrier functions provide a systematic method to synthesize controllers that guarantee forward invariance of safe sets and convergence to transition boundaries. This design-for-verification approach reduces the likelihood that interface complexity becomes insurmountable. Focusing verification effort on expulsory modes—where safety is most critical—allows more complex analysis to be applied selectively rather than uniformly across all modes, concentrating computational resources where they matter most for safety assurance.

5.3 Procedure Formalization Completeness

The third assumption is that existing startup procedures contain sufficient detail and clarity for translation into temporal logic specifications. Nuclear operating procedures, while extensively detailed, were written for human operators who bring contextual understanding and adaptive reasoning to their interpretation. Procedures may contain implicit knowledge, ambiguous directives, or references to operator judgment that resist formalization in current specification languages. Underspecified timing constraints, ambiguous condition definitions, or gaps in operational coverage would cause synthesis to fail or produce incorrect automata. The risk is not merely that formalization is difficult, but that current procedures fundamentally lack the precision required for autonomous control, revealing a gap between human-oriented documentation and machine-executable specifications.

Several indicators would reveal formalization completeness problems early in the project. FRET realizability checks failing due to underspecified behaviors or conflicting requirements would indicate procedures do not form a complete specification. Multiple valid interpretations of procedural steps with no clear resolution would demonstrate procedure language is insufficiently precise for automated synthesis. Procedures referencing "operator judgment," "as appropriate," or similar discretionary language for critical decisions would explicitly identify points where human reasoning cannot be directly formalized. Domain experts unable to provide crisp answers to specification questions about edge cases would suggest the procedures themselves do not fully define system behavior, relying instead on operator training and experience to fill gaps.

The contingency plan treats inadequate specification as itself a research contribution rather than a project failure. Documenting specific ambiguities encountered would create a taxonomy of formalization barriers: timing underspecification, missing preconditions, discretionary actions, and undefined failure modes. Each category would be analyzed to understand why current procedure-writing practices produce these gaps and what specification languages would need to address them. Proposed extensions to FRETish or similar specification languages would demonstrate how to bridge the gap between current procedures and the precision needed for autonomous control. The research output would shift from "here is a complete autonomous controller" to "here is what formal autonomous control requires that current procedures do not provide, and here are language extensions to bridge that gap." This contribution remains valuable to both the nuclear industry and formal methods community, establishing clear requirements for next-generation procedure development and autonomous control specification languages.

Early-stage procedure analysis with domain experts provides the primary mitigation strategy. Collaboration through the University of Pittsburgh Cyber Energy Center enables identification and resolution of ambiguities before synthesis attempts, rather than discovering them during failed synthesis runs. Iterative refinement with reactor operators and control engineers can clarify procedural intent before formalization begins, reducing the risk of discovering insurmountable specification gaps late in the project. Comparison with procedures from multiple reactor designs—pressurized water reactors, boiling water reactors, and advanced designs—may reveal common patterns and standard ambiguities amenable to systematic resolution. This cross-design analysis would strengthen the generalizability of any proposed specification language extensions, ensuring they address industry-wide practices rather than specific quirks.

6 Broader Impacts

Nuclear power presents both a compelling application domain and an urgent economic challenge. Recent interest in powering artificial intelligence infrastructure has renewed focus on small modular reactors (SMRs), particularly for hyperscale datacenters requiring hundreds of megawatts of continuous power. Deploying SMRs at datacenter sites would minimize transmission losses and eliminate emissions from hydrocarbon-based alternatives. However, nuclear power economics at this scale demand careful attention to operating costs.

According to the U.S. Energy Information Administration's Annual Energy Outlook 2022, advanced nuclear power entering service in 2027 is projected to cost \$88.24 per megawatt-hour [24]. Datacenter electricity demand is projected to reach 1,050 terawatt-hours annually by 2030 [25]. If this demand were supplied by nuclear power, the total annual cost of power generation would exceed \$92 billion. Within this figure, operations and maintenance represents a substantial component. The EIA estimates that fixed O&M costs alone account for \$16.15 per megawatt-hour, with additional variable O&M costs embedded in fuel and operating expenses [24]. Combined, O&M-related costs represent approximately 23–30% of the total levelized cost of electricity, translating to \$21–28 billion annually for projected datacenter demand.

This research directly addresses the multi-billion-dollar O&M cost challenge through high-assurance autonomous control. Current nuclear operations require full control room staffing for each reactor, whether large conventional units or small modular designs. These staffing requirements drive the high O&M costs that make nuclear power economically challenging, particularly for smaller reactor designs where the same staffing overhead must be spread across lower power output. Synthesizing provably correct hybrid controllers from formal specifications can automate routine operational sequences that currently require constant human oversight. This enables a fundamental shift from direct operator control to supervisory monitoring, where operators oversee multiple autonomous reactors rather than manually controlling individual units.

The correct-by-construction methodology is critical for this transition. Traditional automation approaches cannot provide sufficient safety guarantees for nuclear applications, where regulatory requirements and public safety concerns demand the highest levels of assurance. Formally verifying both the discrete mode-switching logic and the continuous control behavior, this research will produce controllers with mathematical proofs of correctness. These guarantees enable automation to safely handle routine operations—startup sequences, power level changes, and normal operational transitions—that currently require human operators to follow written procedures. Operators will remain in supervisory roles to handle off-normal conditions and provide authorization for major operational changes, but the routine cognitive burden of procedure execution shifts to provably correct automated systems that are much cheaper to operate.

SMRs represent an ideal deployment target for this technology. Nuclear Regulatory Commission certification requires extensive documentation of control procedures, operational requirements, and safety analyses written in structured natural language. As described in our approach, these regulatory documents can be translated into temporal logic specifications using tools like FRET, then synthesized into discrete switching logic using reactive synthesis tools, and finally verified using reachability analysis and barrier certificates for the continuous control modes. The infrastructure of requirements and specifications already exists as part of the licensing process, creating a direct pathway from existing regulatory documentation to formally verified autonomous controllers.

Beyond reducing operating costs for new reactors, this research will establish a generalizable framework for autonomous control of safety-critical systems. The methodology of translating operational procedures into formal specifications, synthesizing discrete switching logic, and verifying continuous mode behavior applies to any hybrid system with documented operational requirements. Potential applications include chemical process control, aerospace systems, and autonomous transportation, where similar economic and safety considerations favor increased autonomy with provable correctness guarantees. Demonstrating this approach in nuclear power—one of the most regulated and safety-critical domains—will establish both the technical feasibility and regulatory pathway for broader adoption across critical infrastructure.

7 Schedule, Milestones, and Deliverables

This research will be conducted over six trimesters (24 months) of full-time effort following the proposal defense in Spring 2026. The work progresses sequentially through three main research thrusts before culminating in integrated demonstration and validation.

The first semester (Spring 2026) focuses on Thrust 1, translating startup procedures into formal temporal logic specifications using FRET. This establishes the foundation for automated synthesis by converting natural language procedures into machine-readable requirements. The second semester (Summer 2026) addresses Thrust 2, using Strix to synthesize the discrete automaton that defines mode-switching behavior. With the discrete structure established, the third semester (Fall 2026) develops the continuous controllers for each operational mode through Thrust 3, employing reachability analysis and barrier certificates to verify that each mode satisfies its transition requirements. Integration and validation occupy the remaining three semesters.

Figure 1 shows the complete project schedule including research thrusts, major milestones, and planned publications.

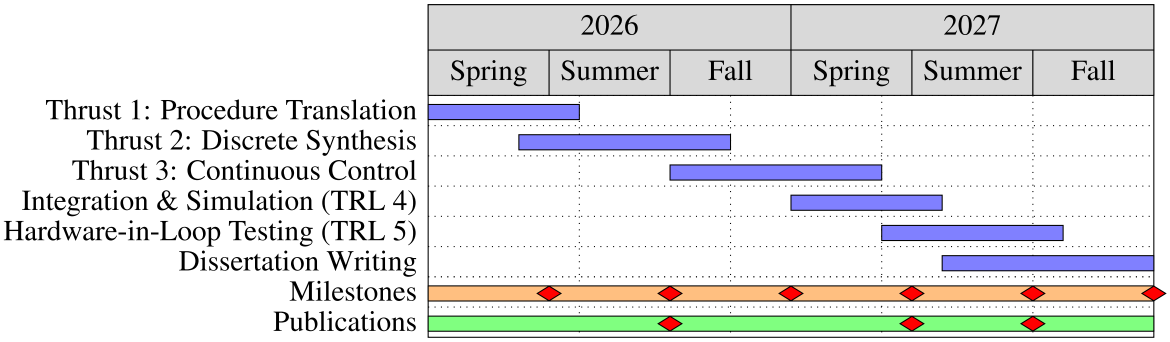

Figure 1: Project schedule showing major research thrusts, milestones (orange row), and publications (green row). Red diamonds indicate completion points. Overlapping bars indicate parallel work where appropriate.

7.1 Milestones and Deliverables

Six major milestones mark critical validation points throughout the research. M1 (Month 4) confirms that startup procedures have been successfully translated to temporal logic using FRET with realizability analysis demonstrating consistent and complete specifications. M2 (Month 8) validates computational tractability by demonstrating that Strix can synthesize a complete discrete automaton from the formalized specifications. This milestone delivers a conference paper submission to NPIC&HMIT documenting the procedure-to-specification translation methodology. M3 (Month 12) achieves TRL 3 by proving that continuous controllers can be designed and verified to satisfy discrete transition requirements. This milestone delivers an internal technical report demonstrating component-level verification. M4 (Month 16) achieves TRL 4 through integrated simulation demonstrating that component-level correctness composes to system-level correctness. This milestone delivers a journal paper submission to IEEE Transactions on Automatic Control presenting the complete hybrid synthesis methodology. M5 (Month 20) achieves TRL 5 by demonstrating practical implementability on industrial hardware. This milestone delivers a conference paper submission to NPIC&HMIT or CDC documenting hardware implementation and experimental validation. M6 (Month 24) completes the dissertation documenting the entire methodology, experimental results, and research contributions.

References

[1] U.S. Nuclear Regulatory Commission, “Guidelines for the preparation of emergency operating procedures,” Tech. Rep. NUREG-0899, U.S. Nuclear Regulatory Commission, 1982.

[2] U.S. Nuclear Regulatory Commission, “10 CFR Part 50.34.” Code of Federal Regulations.

[3] U.S. Nuclear Regulatory Commission, “10 CFR Part 55.59.” Code of Federal Regulations.

[4] “Westinghouse RPS System Description,” tech. rep., Westinghouse Electric Corporation.

[5] C. D. Gentillon, D. Marksberry, D. Rasmuson, M. B. Calley, S. A. Eide, and T. Wierman, “Westinghouse reactor protection system unavailability, 1984-1995.” Number: INEEL/CON-99-00374 Publisher: Idaho National Engineering and Environmental Laboratory.

[6] U.S. Nuclear Regulatory Commission, “Operator Licensing.” `https://www.nrc.gov/reactors/operator-licensing`.

[7] U.S. Nuclear Regulatory Commission, “Part 55—Operators’ Licenses.” `https://www.nrc.gov/reading-rm/doc-collections/cfr/part055/full-text`.

[8] U.S. Nuclear Regulatory Commission, “§ 50.54 Conditions of Licenses.” `https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0054`.

[9] J. G. Kemeny *et al.*, “Report of the president’s commission on the accident at three mile island,” tech. rep., President’s Commission on the Accident at Three Mile Island, October 1979.

[10] World Nuclear Association, “Safety of nuclear power reactors.” `https://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/safety-of-nuclear-power-reactors.aspx`, 2020.

[11] L. Högberg, “Root causes and impacts of severe accidents at large nuclear power plants,” vol. 42, no. 3, pp. 267–284.

[12] M. Zhang, L. Dai, W. Chen, and E. Pang, “Analysis of human errors in nuclear power plant event reports,” vol. 57, no. 10, p. 103687.

[13] J. Kiniry, A. Bakst, S. Hansen, M. Podhradsky, and A. Bivin, “High assurance rigorous digital engineering for nuclear safety (hardens) final technical report,” Tech. Rep. TLR-RES-RES/DE-2024-005, Galois, Inc. / U.S. Nuclear Regulatory Commission, 2024. NRC Contract 31310021C0014.

[14] A. Katis, A. Mavridou, D. Giannakopoulou, T. Pressburger, and J. Schumann, “Capture, analyze, diagnose: Realizability checking of requirements in FRET,” in *Computer Aided Verification* (S. Shoham and Y. Vizel, eds.), pp. 490–504, Springer International Publishing.

[15] C. Baier and J.-P. Katoen, *Principles of Model Checking*. MIT Press.

[16] P. J. Meyer, S. Sickert, and M. Luttenberger, "Strix: Explicit reactive synthesis strikes back!," in *Computer Aided Verification* (H. Chockler and G. Weissenbacher, eds.), pp. 578–586, Springer International Publishing.

[17] S. Jacobs *et al.*, "The reactive synthesis competition (SYNTCOMP): 2018-2021."

[18] M. Branicky, "Multiple lyapunov functions and other analysis tools for switched and hybrid systems," vol. 43, no. 4, pp. 475–482.

[19] S. Bansal, M. Chen, S. Herbert, and C. J. Tomlin, "Hamilton-jacobi reachability: A brief overview and recent advances," in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pp. 2242–2253.

[20] C. L. Guernic, "Reachability analysis of hybrid systems with linear continuous dynamics."

[21] G. Frehse, C. Le Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler, "SpaceEx: Scalable verification of hybrid systems," in *Computer Aided Verification* (G. Gopalakrishnan and S. Qadeer, eds.), pp. 379–395, Springer.

[22] I. Mitchell, A. Bayen, and C. Tomlin, "A time-dependent hamilton-jacobi formulation of reachable sets for continuous dynamic games," vol. 50, no. 7, pp. 947–957.

[23] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *Hybrid Systems: Computation and Control* (R. Alur and G. J. Pappas, eds.), pp. 477–492, Springer.

[24] U.S. Energy Information Administration, "Levelized costs of new generation resources in the annual energy outlook 2022," report, U.S. Energy Information Administration, March 2022. See Table 1b, page 9.

[25] Environmental and Energy Study Institute, "Data center energy needs are upending power grids and threatening the climate." Web article, 2024. Accessed: 2025-09-29.

8 Budget and Budget Justification

8.1 Budget Summary

The proposed research will be conducted over three (3) years, corresponding to the expected completion timeline for the PhD dissertation. Table 1 provides a detailed breakdown of costs by category and year.

Table 1: Proposed Budget by Year and Category

Category	**Year 1**	**Year 2**	**Year 3**	**Total**
Senior Personnel				
Faculty (PI Advisor, 1 mo.)	$12,083	$12,566	$13,069	$37,718
Other Personnel				
Graduate Research Assistant	$38,000	$39,520	$41,101	$118,621
Fringe Benefits				
Faculty Fringe Benefits (29.6%)	$3,577	$3,720	$3,868	$11,165
GRA Fringe Benefits (50%)	$19,000	$19,760	$20,551	$59,311
Fringe Benefits Subtotal	$22,577	$23,480	$24,419	$70,476
Equipment				
(No equipment over $5,000)	—	—	—	—
Travel				
Conference Travel (Domestic)	$4,000	$4,000	$4,000	$12,000
Industry Collaboration Visits	$1,500	$1,500	$1,500	$4,500
Travel Subtotal	$5,500	$5,500	$5,500	$16,500
Participant Support Costs				
(Not applicable)	—	—	—	—
Other Direct Costs				
Materials and Supplies:				
High-Performance Workstation	$3,500	—	—	$3,500
Laboratory Materials & Supplies	$1,500	$1,000	$1,000	$3,500
Publication Costs	$1,000	$1,500	$2,000	$4,500
Computing/Cloud Services	$1,500	$1,500	$1,500	$4,500
Other Direct Costs Subtotal	$7,500	$4,000	$4,500	$16,000
Total Direct Costs	$85,660	$85,066	$88,589	$259,315
H. Indirect Costs (F&A)				
On-Campus Research (56% MTDC)	$35,326	$34,488	$35,935	$105,749
TOTAL PROJECT COST	$120,986	$119,554	$124,524	$365,064

8.2 Budget Justification

8.2.1 Senior Personnel

Faculty Advisor Funds are requested to support one month of summer salary per year for the faculty advisor (estimated at Associate Professor level, $96,459/year base salary for 8 academic months = $12,083/month). A 4% annual salary increase is applied in subsequent years.

8.2.2 Other Personnel

Graduate Research Assistant (Principal Investigator) Funds are requested to support one full-time graduate research assistant (the PI) for the entire duration of the project at $38,000 per year in Year 1. This represents a standard graduate research assistantship stipend at the University of Pittsburgh for a PhD student in the Swanson School of Engineering. A 4% annual salary increase is included in Years 2 and 3 to account for cost-of-living adjustments.

8.2.3 Fringe Benefits

Faculty Fringe Benefits Faculty fringe benefits are calculated at 29.6%, the University of Pittsburgh's approved rate for academic year faculty, covering retirement contributions, health insurance, and other benefits.

Graduate Research Assistant Fringe Benefits Fringe benefits for the GRA are calculated at 50% of salary, consistent with University of Pittsburgh rates for graduate students on research assistantships.

8.2.4 Travel

Conference Travel ($4,000 per year) Funds are requested for the PI and faculty advisor to attend one major control systems conference annually to disseminate research results. The budget assumes domestic conference attendance with costs including: airfare, hotel, meals and incidentals, ground transportation, and registration for both attendees per conference.

Industry Collaboration Visits ($1,500 per year) Funds are requested for travel to industry partner sites and potential nuclear facilities to: (1) validate reactor operating procedures with domain experts; (2) present research progress to industry stakeholders; (3) gather feedback on practical implementation considerations; and (4) explore deployment pathways for the developed technology.

8.2.5 Other Direct Costs

Materials and Supplies *High-Performance Workstation ($3,500, Year 1):* A dedicated high-performance workstation is required for computationally intensive tasks including. The workstation specifications include: Intel Core i9 or AMD Ryzen 9 processor (minimum 16 cores), 64 GB RAM, 2 TB NVMe SSD storage, and NVIDIA GPU for potential acceleration of numerical computations.

Laboratory Materials and Supplies ($1,500 Year 1; $1,000 Years 2–3): Funds are requested for laboratory supplies and materials including: electronic components and sensors for hardware integration, cables and connectors for hardware-in-the-loop setup, and miscellaneous computing accessories such as external storage devices and backup media.

Publication Costs Funds are requested to cover publication fees for disseminating research results in high-quality peer-reviewed venues. Budget includes:

- Year 1 ($1,000): Conference proceedings fees and one journal submission

- Year 2 ($1,500): Open-access publication charges for first major journal paper
- Year 3 ($2,000): Open-access publication charges for dissertation-culminating journal papers

Open-access publication is prioritized to maximize research impact and accessibility, particularly important for work with potential nuclear safety applications. Many high-impact journals (IEEE Transactions on Automatic Control, Automatica) charge $1,000–$2,000 for open access.

Computing and Cloud Services Funds are requested for cloud computing resources and online services. Cloud computing provides scalable computational resources for particularly demanding verification problems without requiring additional capital equipment purchases.

8.2.6 H. Indirect Costs (Facilities & Administrative)

Indirect costs are calculated at 56% of Modified Total Direct Costs (MTDC), which is the University of Pittsburgh's federally negotiated rate for on-campus research. MTDC includes all direct costs except equipment purchases over $5,000, tuition remission, and certain other exclusions. The calculation base includes all personnel costs, travel, and other direct costs as shown in the budget table.

9 Supplemental Sections

9.1 Biosketch

IDENTIFYING INFORMATION:

NAME: Sabo, Dane

ORCID iD: https://orcid.org/0009-0003-3594-6728

POSITION TITLE: Graduate Student Researcher

PRIMARY ORGANIZATION AND LOCATION: University of Pittsburgh, Pittsburgh, Pennsylvania, United States

Professional Preparation:

ORGANIZATION AND LOCATION	DEGREE (if applicable)	RECEIPT DATE	FIELD OF STUDY
University of Pittsburgh, Pittsburgh, Pennsylvania, United States	Doctor of Philosophy	08/2027	Mechanical Engineering
University of Pittsburgh, Pittsburgh, Pennsylvania, US	Bachelors of Science	08/2023	Mechanical Engineering

Appointments and Positions

2023 - 2027	Graduate Student Researcher, University of Pittsburgh, Pittsburgh, Pennsylvania, United States
2022 - 2023	Independent Contractor (Mechanical Engineer), Human Motion Technologies, Pittsburgh, Pennsylvania, United States
2022 - 2022	Content Developer and Teaching Assistant, University of Pittsburgh, Mechanical Engineering, Pittsburgh, Pennsylvania, US
2022 - 2022	Undergraduate Research Intern, University of Pittsburgh, Mechanical Engineering And Materials Science Department, Pittsburgh, Pennsylvania, US
2021 - 2021	Mechanical Engineering Co-Op, BMW Manufacturing, TX-5, Greer, South Carolina, US

Products

Products Most Closely Related to the Proposed Project

1. Robert Lois, Dane Sabo, Patrick Murphy, Luis Benitez, Daniel Cole. Employing a Hardware-in-the-Loop Approach to Realize a Fully Homomorphic Encrypted Controller for a Small Modular Advanced High Temperature Reactor. Nuclear Plant Instrumentation and Control &amp; Human-Machine Interface Technology (NPIC&amp;HMIT 2025); ; c2025. DOI: 10.13182/xyz-46729

Other Significant Products, Whether or Not Related to the Proposed Project

Certification:

I certify that the information provided is current, accurate, and complete. This includes but is not limited to information related to domestic and foreign appointments and positions.

I also certify that, at the time of submission, I am not a party to a malign foreign talent recruitment program.

Misrepresentations and/or omissions may be subject to prosecution and liability pursuant to, but not limited to, 18 U.S.C. §§ 287, 1001, 1031 and 31 U.S.C. §§ 3729-3733 and 3802.

Certified by Sabo, Dane in SciENcv on 2025-11-17 09:05:50

9.2 Data Management Plan

High Assurance Autonomous Control Systems

Data sharing and preservation

Data management plans should describe whether and how data generated in the course of the proposed research will be shared and preserved and, at a minimum, describe how data sharing and preservation will enable validation of results, or how results could be validated if data are not shared or preserved.

This research will generate formal specifications (temporal logic), discrete automata models, continuous controller implementations, simulation data from SmAHTR models, and hardware-in-the-loop validation results. Digital research data necessary to validate findings include: synthesized controller code, FRET requirement specifications, Simulink reactor models, and experimental performance metrics.

All code will be documented following standard software engineering practices with inline comments and README files. Controller specifications will use FRET and temporal logic formats compatible with reactive synthesis tools. Simulation data will be stored in CSV format with accompanying metadata describing experimental conditions.

All research artifacts will be published in a public GitHub repository under an open-source license immediately upon publication of research findings. The repository will remain publicly accessible indefinitely through GitHub's standard preservation policies. No proprietary software is required for data access.

Open access to controller synthesis methodologies and validated implementations will accelerate adoption of formal methods in nuclear control systems and enable reproducibility of safety-critical autonomous control research.

Data used in publications

Data management plans should provide a plan for making all research data displayed in publications resulting from the proposed research open, machine-readable, and digitally accessible to the public at the time of publication. This includes data that are displayed in charts, figures, images, etc. In addition, the underlying digital research data used to generate the displayed data should be made as accessible as possible to the public in accordance with the Principles published in the DOE Policy for Digital Research Data Management. The published article should indicate how these data can be accessed.

All data displayed in charts, figures, and images in publications will be made publicly available in machine-readable formats (CSV, JSON) in the project's GitHub repository at the time of publication. Underlying digital research data used to generate all visualizations and results will be included with comprehensive metadata. LaTeX source files for papers will also be published to enable full reproducibility. Each publication will include a data availability statement with direct links to the corresponding datasets and source files in the repository.

Data management resources

Data management plans should consult and reference available information about data management resources to be used in the course of the proposed research. In particular, DMPs that explicitly or implicitly commit data management resources at a facility beyond what is conventionally made available to approved users should be accompanied by written approval from that facility. In determining the resources available for data management at DOE Scientific User Facilities, researchers should consult the published description of data management resources and practices at that facility and reference it in the DMP.

This research will utilize standard computational and data management resources provided by the University of Pittsburgh Cyber Energy Center, including local computing infrastructure for simulation and data storage. Hardware-in-the-loop testing will use Emerson Ovation control equipment already available at the Center for approved research use. All data management activities fall within conventional resource allocations for approved users and do not require additional commitments beyond standard laboratory access. No DOE Scientific User Facilities will be utilized for data management.

Confidentiality, security and rights

Data management plans must protect confidentiality, personal privacy, Personally Identifiable Information and U.S. national, homeland, and economic security; recognize propriety interests, business confidential information, and intellectual property rights; avoid significant negative impact on innovation and U.S. competitiveness; and otherwise be consistent with all applicable laws, regulations, agreement terms and conditions, and DOE orders and policies.

This research involves no collection or processing of Personally Identifiable Information. All published data will be reviewed to ensure compliance with export control regulations and nuclear security requirements before public release. Any proprietary information from industry partners (e.g., Emerson control system specifications) will be excluded from public repositories or shared only with appropriate written permission. Controller implementations will be published at a methodological level that advances scientific knowledge while avoiding disclosure of sensitive facility-specific details that could impact national or homeland security. All data management practices will comply with applicable DOE orders, export control laws, and university intellectual property policies.

Planned Research Outputs

Model representation - "Controller Proof Artifacts"

All artifacts created in the process of generating a hybrid autonomous controller will be disseminated, including all intermediate representations. These include formal specifications in FRETtish, hybrid automata in the form of .dot files, and finally built controllers in the form of Simulink models.

Planned research output details

Title	Type	Anticipated release date	Initial access level	Intended repository(ies)	Anticipated file size	License	Metadata standard(s)	May contain sensitive data?	May contain PII?
Controller Proof Artifacts	Model representation	2027-08-30	Open	None specified		None specified	None specified	No	No

9.3 Facilities

University of Pittsburgh Cyber Energy Center. This research will be conducted at the Cyber Energy Center, a specialized facility dedicated to advancing cybersecurity and control systems for critical energy infrastructure. The Center provides access to industry-standard control equipment, including Emerson Ovation distributed control systems representative of modern nuclear plant instrumentation and control platforms. The Center maintains active collaborations with industry partners, enabling real-world validation of research outcomes and ensuring alignment with practical deployment requirements. Hardware-in-the-loop testing capabilities include the Advanced Reactor Cyber Analysis and Development Environment (ARCADE) suite for real-time integration between simulation models and physical control hardware.

Center for Research Computing (CRC). The CRC provides high-performance computing resources essential for computationally intensive verification tasks including reachability analysis, barrier certificate computation, and large-scale reactor simulations. The Center maintains multi-node computing clusters with parallel processing capabilities, GPU acceleration for neural network-based verification approaches, and substantial data storage infrastructure. Technical support staff provide expertise in scientific computing, enabling efficient utilization of computational resources for formal methods applications.

Swanson School of Engineering. The Mechanical Engineering and Materials Science Department within the Swanson School provides comprehensive facilities for engineering research including computational laboratories, collaborative workspaces, and access to software licenses for MATLAB/Simulink, control system design tools, and formal verification platforms. The School's emphasis on interdisciplinary research creates opportunities for collaboration across control systems, computer science, and nuclear engineering domains essential to this hybrid control synthesis methodology.