Formally Verified Autonomous Hybrid Control

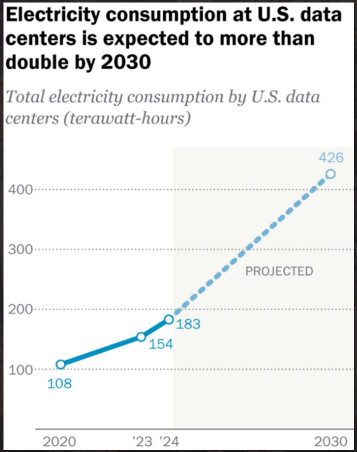
Dane A. Sabo
dane.sabo@pitt.edu

Dr. Daniel G. Cole
dgcole@pitt.edu

University of Pittsburgh

November 29, 2025

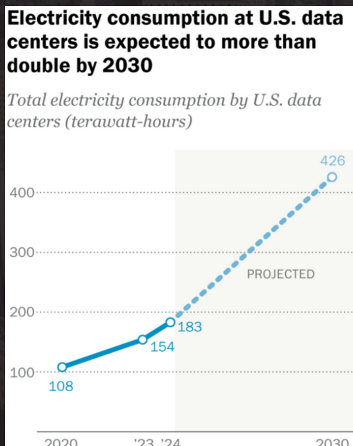
The United States stands on the precipice of a severe energy crises



Source: Pew Research Center, Data from IEA

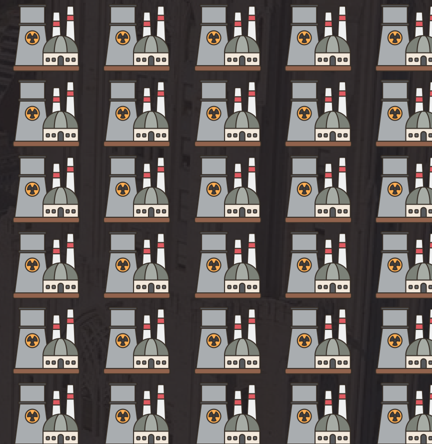
How much baseload power increase is this?

The United States stands on the precipice of a severe energy crises



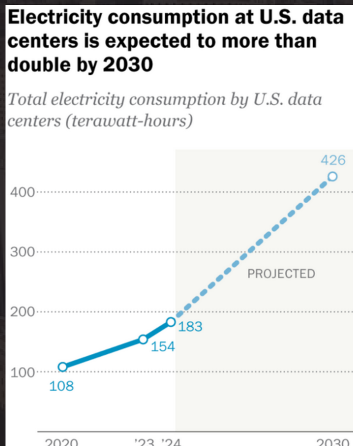
Source: Pew Research Center, Data from IEA

How much baseload power increase is this?



30 gigawatts!

The United States stands on the precipice of a severe energy crises



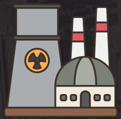
Source: Pew Research Center, Data from IEA

How much baseload power increase is this?

30 gigawatts!

Staffing these new reactors will be an incredible challenge

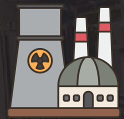
How many reactor operators are required to staff this new fleet?



For one Small Modular Reactor (SMR)...

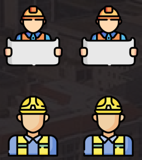
Staffing these new reactors will be an incredible challenge

How many reactor operators are required to staff this new fleet?



For one Small Modular Reactor (SMR)...

One shift requires:



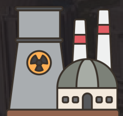
2 Senior Reactor Operators

2 Reactor Operators

University of Pittsburgh
Cyber Energy Center

Staffing these new reactors will be an incredible challenge

How many reactor operators are required to staff this new fleet?



For one Small Modular Reactor (SMR)...

24/7 operations require ∼6 shifts:

12 SROs

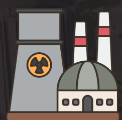
12 ROs

24 licensed operators per reactor

University of Pittsburgh
Cyber Energy Center

Staffing these new reactors will be an incredible challenge

How many reactor operators are required to staff this new fleet?



For one Small Modular Reactor (SMR)...

24/7 operations require ∼6 shifts:

12 SROs

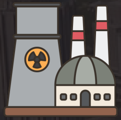
12 ROs

24 licensed operators per reactor

To meet demand we require 2,400 new licensed operators!

Staffing these new reactors will be an incredible challenge

How many reactor operators are required to staff this new fleet?



For one Small Modular Reactor (SMR)...

24/7 operations require ∼6 shifts:

12 SROs

12 ROs

24 licensed operators per reactor

To meet demand we require 2,400 new licensed operators!

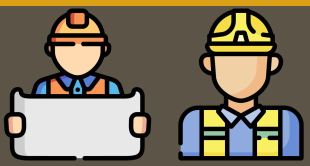
We currently have only 3,600 licensed operators total...

University of Pittsburgh
Cyber Energy Center

Nuclear reactors are operated with prescriptive handbooks

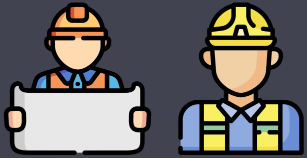
Human reactor operators have key limitations that limit nuclear buildout

Humans cannot meet labor demand



Human reactor operators have key limitations that limit nuclear buildout

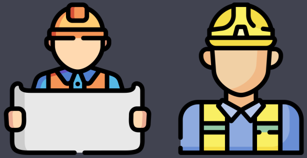
Humans cannot meet labor demand



Procedures are not exhaustively verified

Human reactor operators have key limitations that limit nuclear buildout

Humans cannot meet labor demand



Procedures are not exhaustively verified

Human factors cannot be trained away

The goal of this research is to create verified autonomous control systems

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

University of Pittsburgh
Cyber Energy Center

The goal of this research is to create verified autonomous control systems

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

1. Translate written procedures into discrete control logic

University of Pittsburgh
Cyber Energy Center

The goal of this research is to create verified autonomous control systems

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

1. Translate written procedures into discrete control logic
2. Verify continuous control behavior across discrete mode transitions

University of Pittsburgh
Cyber Energy Center

The goal of this research is to create verified autonomous control systems

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

1. Translate written procedures into discrete control logic
2. Verify continuous control behavior across discrete mode transitions
3. Demonstrate autonomous reactor startup with verifiable safety guarantees

University of Pittsburgh
Cyber Energy Center

First, we will formalize written procedures into logical statements

APPENDIX 19-1
Plant Startup from Cold Shutdown

I. INITIAL CONDITIONS

1. Cold Shutdown - MODE 5:
   - $K_{eff} < 0.99$
   - 0% power
   - $T_{avg} < 200°F$
2. Reactor Coolant System: solid.
3. RCS Temperature: 150 - 160°F.

Note:
Temperature may be less than 150°F depending upon the decay heat load of the core.

4. RCS Pressure: 320 - 400 psig.
5. Steam Generators: filled to wet layup (100% wide-range level indication).
6. Secondary Systems: shutdown, main turbine and feedwater pump turbines on their turning gears.
7. Pre-Startup Checklists: completed.

II. INSTRUCTIONS

A. Heatup from COLD SHUTDOWN to HOT SHUTDOWN (MODE 5 to MODE 4)

1. Permission received from Operations Supervisor for startup.
2. Begin establishing steam generator water levels to 33 ± 5% narrow-range indication.
3. Verify or establish RCP seal injection flow.

CAUTION:
Do not exceed a heatup rate of 100°F/hr in the pressurizer or 100°F/hr in the RCS. Do not exceed 320°F ΔT between pressurizer and spray temperature. Use auxiliary spray for pressurizer volume and coolant mixing.

4. Energize pressurizer heaters and begin pressurizer heatup.
5. Establish a pressurizer steam bubble by;
   a. Increasing pressurizer temperature using pressurizer heaters.
   b. Adjust charging and letdown flow to maintain pressurizer pressure at approximately 320-400 psig while reducing pressurizer level.
   c. As pressurizer temperature approaches 428°F (saturation temperature for 320 psig), reduce pressurizer level toward 25%.

First, we will formalize written procedures into logical statements

APPENDIX 19-1
Plant Startup from Cold Shutdown

I. INITIAL CONDITIONS

1. Cold Shutdown - MODE 5:
   - K_{eff} < 0.99
   - 0% power
   - T_{avg} < 200°F
2. Reactor Coolant System: solid.
3. RCS Temperature: 150 - 160°F.

Note:
Temperature may be less than 150°F depending upon the decay heat load of the core.

4. RCS Pressure: 320 - 400 psig.
5. Steam Generators: filled to wet layup (100% wide-range level indication).
6. Secondary Systems: shutdown, main turbine and feedwater pump turbines on their turning gears.
7. Pre-Startup Checklists: completed.

II. INSTRUCTIONS

A. Heatup from COLD SHUTDOWN to HOT SHUTDOWN (MODE 5 to MODE 4)

1. Permission received from Operations Supervisor for startup.
2. Begin establishing steam generator water levels to 33 ± 5% narrow-range indication.
3. Verify or establish RCP seal injection flow.

CAUTION:
Do not exceed a heatup rate of 100°F/hr in the pressurizer or 100°F/hr in the RCS. Do not exceed 320°F ΔT between pressurizer and spray temperature. Use auxiliary spray for pressurizer volume and coolant mixing.

4. Energize pressurizer heaters and begin pressurizer heatup.
5. Establish a pressurizer steam bubble by;
   a. Increasing pressurizer temperature using pressurizer heaters.
   b. Adjust charging and letdown flow to maintain pressurizer pressure at approximately 320-400 psig while reducing pressurizer level.
   c. As pressurizer temperature approaches 428°F (saturation temperature for 320 psig), reduce pressurizer level toward 25%.

USNRC HRTD 19-12 Rev 0109

FRET Specification

```
INITIAL_CONDITIONS shall satisfy:
        mode = MODE_5
        k_eff < 0.99
        power = 0
        t_avg < 200
        ...
```

University of Pittsburgh
Cyber Energy Center

First, we will formalize written procedures into logical statements

APPENDIX 19-1
Plant Startup from Cold Shutdown

I. INITIAL CONDITIONS

1. Cold Shutdown - MODE 5:
   - $K_{eff} < 0.99$
   - 0% power
   - $T_{avg} < 200°F$
2. Reactor Coolant System: solid.
3. RCS Temperature: 150 - 160°F.

> **Note:**
> *Temperature may be less than 150°F depending upon the decay heat load of the core.*

4. RCS Pressure: 320 - 400 psig.
5. Steam Generators: filled to wet layup (100% wide-range level indication).
6. Secondary Systems: shutdown, main turbine and feedwater pump turbines on their turning gears.
7. Pre-Startup Checklists: completed.

II. INSTRUCTIONS

A. Heatup from COLD SHUTDOWN to HOT SHUTDOWN (MODE 5 to MODE 4)

1. Permission received from Operations Supervisor for startup.
2. Begin establishing steam generator water levels to 33 ± 5% narrow-range indication.
3. Verify or establish RCP seal injection flow.

> **CAUTION:**
> *Do not exceed a heatup rate of 100°F/hr in the pressurizer or 100°F/hr in the RCS. Do not exceed 320°F ΔT between pressurizer and spray temperature. Use auxiliary spray for pressurizer volume and coolant mixing.*

4. Energize pressurizer heaters and begin pressurizer heatup.
5. Establish a pressurizer steam bubble by;
   a. Increasing pressurizer temperature using pressurizer heaters.
   b. Adjust charging and letdown flow to maintain pressurizer pressure at approximately 320-400 psig while reducing pressurizer level.
   c. As pressurizer temperature approaches 428°F (saturation temperature for 320 psig), reduce pressurizer level toward 25%.

USNRC HRTD 19-12 Rev 0109

FRET Specification

```
INITIAL_CONDITIONS shall satisfy:
      mode = MODE_5
      k_eff < 0.99
      power = 0
      t_avg < 200
      ...
```

LTL Formula

```
□ (initial → (
      mode = MODE_5 ∧
      k_eff < 0.99 ∧
      power = 0 ∧
      t_avg < 200 ∧
      ...))
```

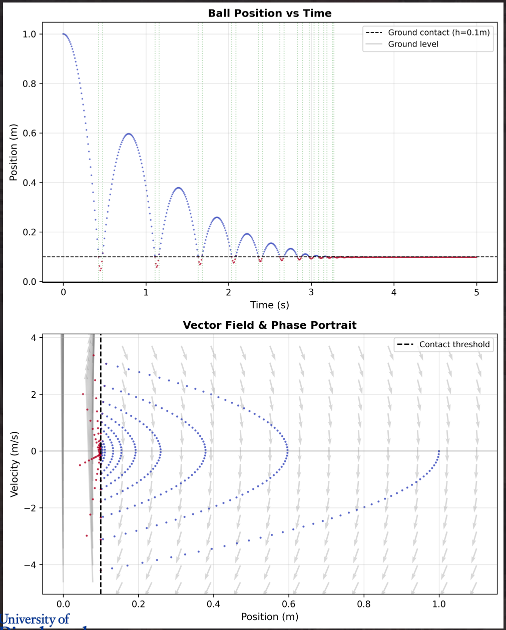
University of Pittsburgh
Cyber Energy Center

Second, we will use the logical formulae to generate discrete automata

LTL Specification → Game Graph → Discrete Automata

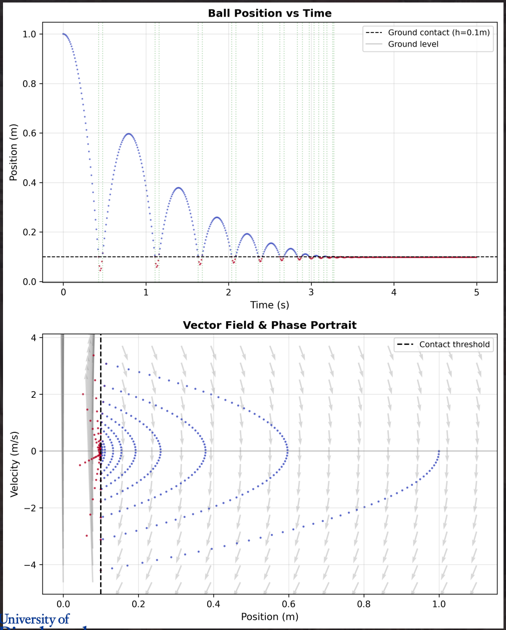
$\underbrace{\text{LTL Specification} \rightarrow \text{Game Graph} \rightarrow \text{Discrete Automata}}_{\textbf{Reactive Synthesis}}$

Finally, we will build continuous controllers to move between discrete states



University of Pittsburgh
Cyber Energy Center

Finally, we will build continuous controllers to move between discrete states

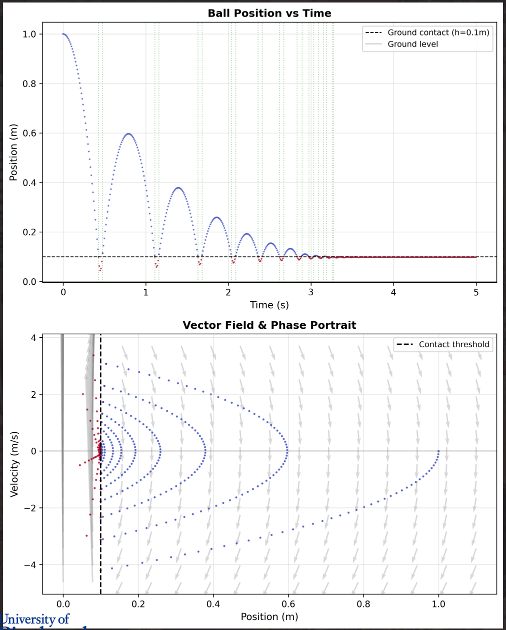


Key Challenge

Verify continuous control behavior across discrete mode transitions

University of Pittsburgh

Finally, we will build continuous controllers to move between discrete states



Key Challenge

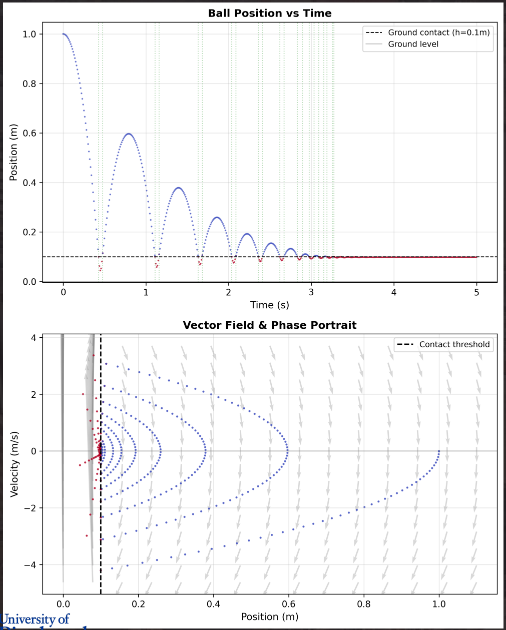
Verify continuous control behavior across discrete mode transitions

Reachable Set

$$\mathcal{R}(t) = \{x(t) \mid x(0) \in X_0, \dot{x} = f(x)\}$$

University of Pittsburgh
Cyber Energy Center

Finally, we will build continuous controllers to move between discrete states



Key Challenge

Verify continuous control behavior across discrete mode transitions

Reachable Set

$\mathcal{R}(t) = \{x(t) \mid x(0) \in X_0, \dot{x} = f(x)\}$

Barrier Certificate

$B(x) > 0 \land \nabla B \cdot f(x) \leq 0 \implies x \in \text{Safe}$

University of Pittsburgh
Cyber Energy Center

Verified autonomous controllers can be created by building this chain of proof of correctness

1. Formalize regulatory procedures into FRET specifications and translate to Linear Temporal Logic (LTL)

Verified autonomous controllers can be created by building this chain of proof of correctness

1. Formalize regulatory procedures into FRET specifications and translate to Linear Temporal Logic (LTL)
2. Synthesize discrete automata from LTL using reactive synthesis

University of Pittsburgh
Cyber Energy Center

Verified autonomous controllers can be created by building this chain of proof of correctness

1. Formalize regulatory procedures into FRET specifications and translate to Linear Temporal Logic (LTL)
2. Synthesize discrete automata from LTL using reactive synthesis
3. Design continuous controllers for each discrete mode and verify safety across mode transitions using barrier certificates and reachability analysis

University of Pittsburgh
Cyber Energy Center

Verified autonomous controllers can be created by building this chain of proof of correctness

1. Formalize regulatory procedures into FRET specifications and translate to Linear Temporal Logic (LTL)
2. Synthesize discrete automata from LTL using reactive synthesis
3. Design continuous controllers for each discrete mode and verify safety across mode transitions using barrier certificates and reachability analysis

Result: Complete hybrid autonomous system with correctness guarantees by construction

University of Pittsburgh
Cyber Energy Center

Success is measured through Technology Readiness Level advancement

Why TRLs?

Bridge gap between academic proof-of-concept and practical deployment

- Academic metrics $\rightarrow$ cannot capture feasibility
- Empirical metrics $\rightarrow$ cannot demonstrate rigor
- TRLs measure both simultaneously

Progression Path

Current: TRL 2-3
Fundamental principles established

Target: TRL 5
Lab testing in relevant environment

TRL advancement requires achieving three validation milestones

1. **TRL 3: Critical Function & Proof of Concept**
   - Each component works in isolation
   - Specifications pass realizability analysis
   - At least one continuous controller with reachability proof

University of Pittsburgh
Cyber Energy Center

TRL advancement requires achieving three validation milestones

1. **TRL 3: Critical Function & Proof of Concept**
   - Each component works in isolation
   - Specifications pass realizability analysis
   - At least one continuous controller with reachability proof
2. **TRL 4: Integrated Components in Simulation**
   - Complete integrated hybrid controller
   - All mode transitions verified
   - Zero safety violations across multiple runs

University of Pittsburgh
Cyber Energy Center

TRL advancement requires achieving three validation milestones

1. **TRL 3: Critical Function & Proof of Concept**
   - Each component works in isolation
   - Specifications pass realizability analysis
   - At least one continuous controller with reachability proof
2. **TRL 4: Integrated Components in Simulation**
   - Complete integrated hybrid controller
   - All mode transitions verified
   - Zero safety violations across multiple runs
3. **TRL 5: Testing in Relevant Environment**
   - Hardware-in-the-loop on Emerson Ovation
   - Autonomous startup sequences via HIL
   - Off-nominal scenarios handled correctly
   - Formal verification remains valid on hardware

University of Pittsburgh
Cyber Energy Center

Four primary risks with clear mitigation and contingency plans

1. **Computational Tractability of Synthesis**

   Risk: Synthesis times exceed project timeline

   Indicator: >24hr for simplified procedures

   Contingency: Reduce to minimal viable startup sequence

   Mitigation: HPC resources, compositional verification

Four primary risks with clear mitigation and contingency plans

1. **Computational Tractability of Synthesis**

   Risk: Synthesis times exceed project timeline

   Indicator: >24hr for simplified procedures

   Contingency: Reduce to minimal viable startup sequence

   Mitigation: HPC resources, compositional verification

2. **Discrete-Continuous Interface Complexity**

   Risk: Boolean guards cannot map to continuous dynamics

   Indicator: No barrier certificates exist for transitions

   Contingency: Restrict to polytopic invariants

   Mitigation: Design controllers with transitions as constraints

University of Pittsburgh
Cyber Energy Center

Four primary risks with clear mitigation and contingency plans

1. **Computational Tractability of Synthesis**
   Risk: Synthesis times exceed project timeline
   Indicator: >24hr for simplified procedures
   Contingency: Reduce to minimal viable startup sequence
   Mitigation: HPC resources, compositional verification
2. **Discrete-Continuous Interface Complexity**
   Risk: Boolean guards cannot map to continuous dynamics
   Indicator: No barrier certificates exist for transitions
   Contingency: Restrict to polytopic invariants
   Mitigation: Design controllers with transitions as constraints
3. **Procedure Formalization Completeness**
   Risk: Procedures lack precision for autonomous control
   Indicator: Multiple valid interpretations, operator judgment
   Contingency: Document gaps as research contribution
   Mitigation: Early analysis with domain experts

University of Pittsburgh
Cyber Energy Center

Four primary risks with clear mitigation and contingency plans

1. **Computational Tractability of Synthesis**
   - *Risk:* Synthesis times exceed project timeline
   - *Indicator:* >24hr for simplified procedures
   - *Contingency:* Reduce to minimal viable startup sequence
   - *Mitigation:* HPC resources, compositional verification
2. **Discrete-Continuous Interface Complexity**
   - *Risk:* Boolean guards cannot map to continuous dynamics
   - *Indicator:* No barrier certificates exist for transitions
   - *Contingency:* Restrict to polytopic invariants
   - *Mitigation:* Design controllers with transitions as constraints
3. **Procedure Formalization Completeness**
   - *Risk:* Procedures lack precision for autonomous control
   - *Indicator:* Multiple valid interpretations, operator judgment
   - *Contingency:* Document gaps as research contribution
   - *Mitigation:* Early analysis with domain experts
4. **Hardware-in-the-Loop Integration**
   - *Risk:* Real-time constraints incompatible with hardware
   - *Indicator:* Communication dropouts, missed deadlines
   - *Contingency:* Software-in-the-loop with timing analysis (TRL 4)

University of Pittsburgh
Cyber Energy Center

Staged structure ensures partial success yields valuable results

Early Detection

Each risk has specific indicators for early warning

- Quarterly assessment of progress
- Data-driven plan revision only when assumptions invalidated

Research Value

Even contingency outcomes contribute knowledge

- Identifying barriers is itself valuable
- Clear pathway for future work
- Publishable results at each stage

Contingency plans preserve core methodology while adjusting scope to maintain feasibility

University of Pittsburgh
Cyber Energy Center