

Formally Verified Autonomous Hybrid Control

Dane A. Sabo

dane.sabo@pitt.edu

Dr. Daniel G. Cole

dgcole@pitt.edu

University of Pittsburgh

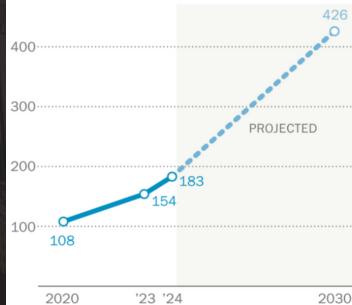
November 30, 2025



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

Electricity consumption at U.S. data centers is expected to more than double by 2030

Total electricity consumption by U.S. data centers (terawatt-hours)



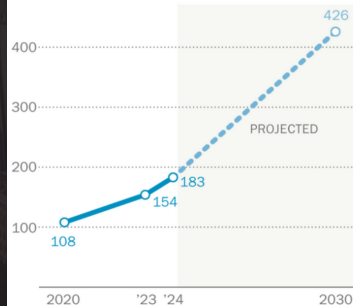
How much baseload power increase is this?

Source: Pew Research Center, Data from IEA

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

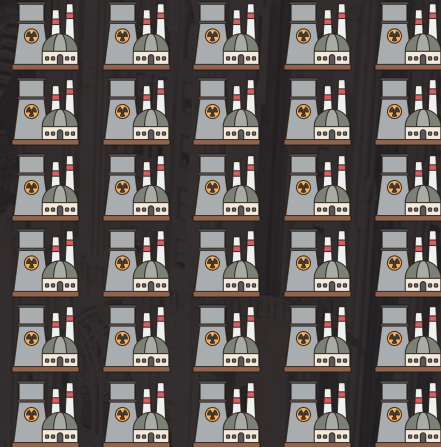
Electricity consumption at U.S. data centers is expected to more than double by 2030

Total electricity consumption by U.S. data centers (terawatt-hours)



Source: Pew Research Center, Data from IEA

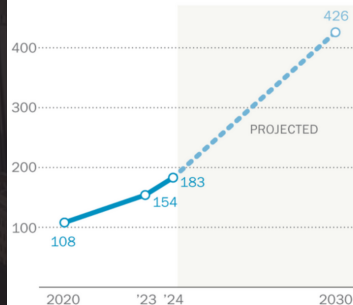
How much baseload power increase is this?



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

Electricity consumption at U.S. data centers is expected to more than double by 2030

Total electricity consumption by U.S. data centers (terawatt-hours)



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)...



2 Senior Reactor Operators



2 Reactor 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

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!

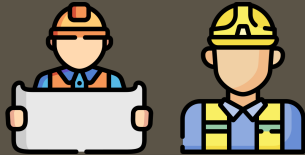
We currently have only 3,600 licensed operators total...

Nuclear reactors are operated with prescriptive handbooks and legacy control technologies



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:

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

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

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

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
- $T_{avg} < 200^{\circ}\text{F}$

2. Reactor Coolant System: solid.
3. RCS Temperature: $150 - 160^{\circ}\text{F}$.

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 $33 \pm 5\%$ 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 $320^{\circ}\text{F } \Delta T$ 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

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
- $T_{avg} < 200^{\circ}\text{F}$

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

$t_{avg} < 200$

...

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
- $T_{avg} < 200^{\circ}\text{F}$

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 layout (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
...
```

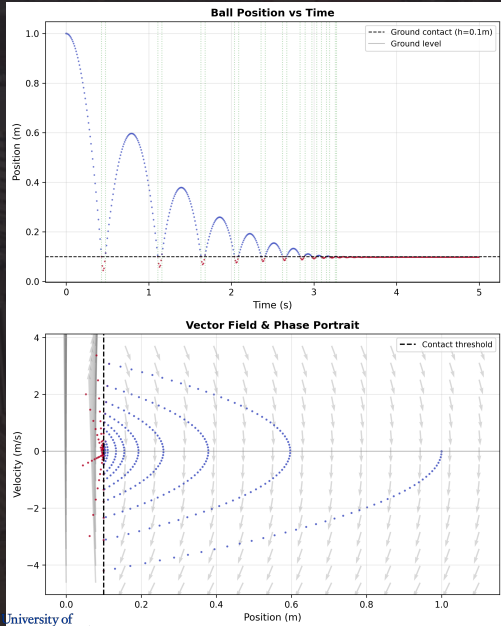
LTL Formula

```
□ (initial → (
    mode_5_active ∧
    k_eff_subcritical ∧
    zero_power ∧
    temp_safe ∧
    ...))
```

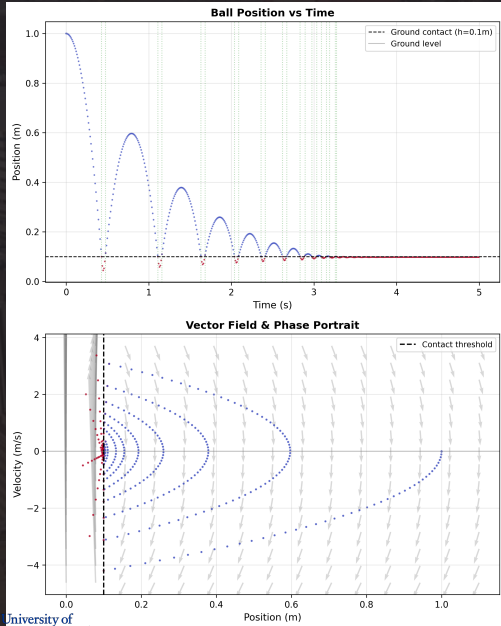
Second, we will use the logical formulae to generate discrete automata



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



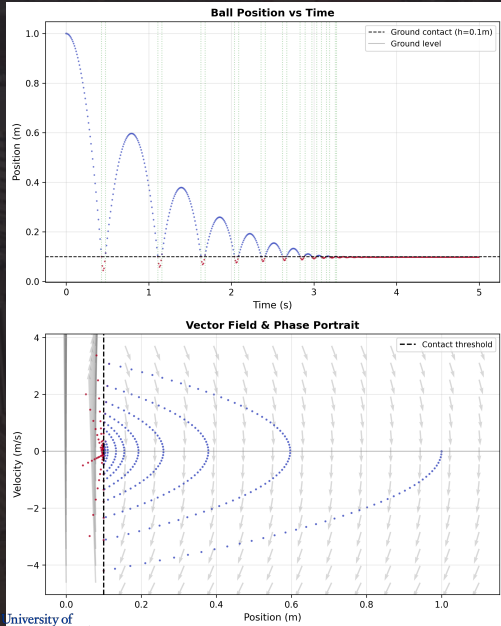
Finally, we will build continuous controllers to move between discrete states



Key Challenge

Verify continuous control behavior across discrete mode transitions

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



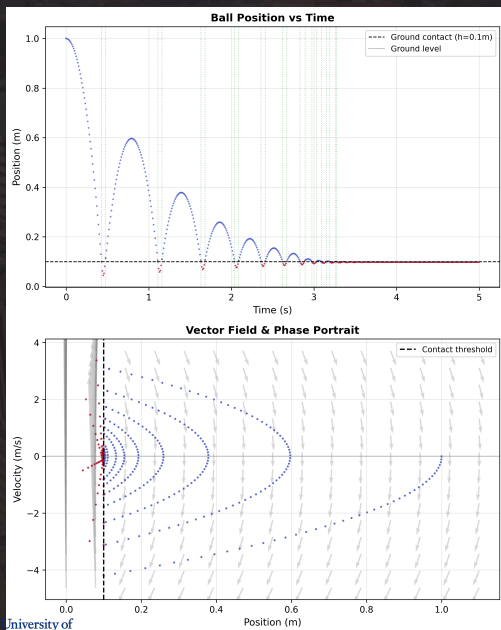
Key Challenge

Verify continuous control behavior across discrete mode transitions

Reachable Set

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

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

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

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

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

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

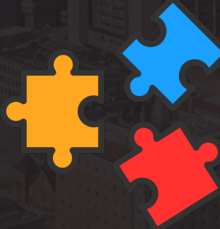
Success will be measured through Technology Readiness Level advancement

Why TRLs?

Bridge gap between proof-of-concept and deployment

Measure both rigor and feasibility

TRL 3
Components



Current: TRL 2-3

Target: TRL 5

Success will be measured through Technology Readiness Level advancement

Why TRLs?

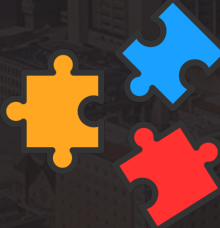
Bridge gap between proof-of-concept and deployment

Measure both rigor and feasibility

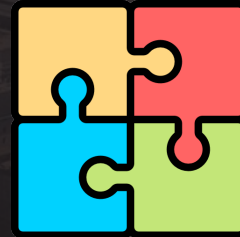
Current: TRL 2-3

Target: TRL 5

TRL 3
Components



TRL 4
Integration



Success will be measured through Technology Readiness Level advancement

Why TRLs?

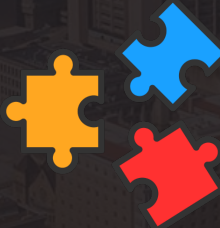
Bridge gap between proof-of-concept and deployment

Measure both rigor and feasibility

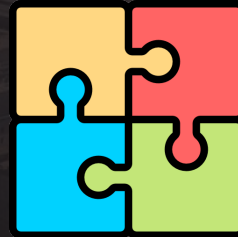
Current: TRL 2-3

Target: TRL 5

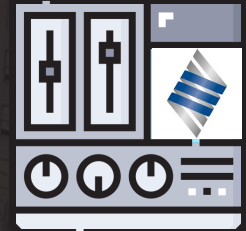
TRL 3
Components



TRL 4
Integration



TRL 5
Hardware



Four primary risks are identified with clear mitigation and contingency plans

1 Computational Tractability of Synthesis

Four primary risks are identified with clear mitigation and contingency plans

- 1 Computational Tractability of Synthesis
- 2 Discrete-Continuous Interface Complexity

Four primary risks are identified with clear mitigation and contingency plans

- 1 Computational Tractability of Synthesis
- 2 Discrete-Continuous Interface Complexity
- 3 Procedure Formalization Completeness

Four primary risks are identified with clear mitigation and contingency plans

- 1 Computational Tractability of Synthesis
- 2 Discrete-Continuous Interface Complexity
- 3 Procedure Formalization Completeness
- 4 Hardware-in-the-Loop Integration

Formally Verified Autonomous Hybrid Control

Enabling Economic Viability
of Next-Generation Nuclear
Power

Dane A. Sabo

dane.sabo@pitt.edu

Advisor:

Dr. Daniel G. Cole

dgcole@pitt.edu

University of Pittsburgh
Department of Mechanical
Engineering and Materials Science

