

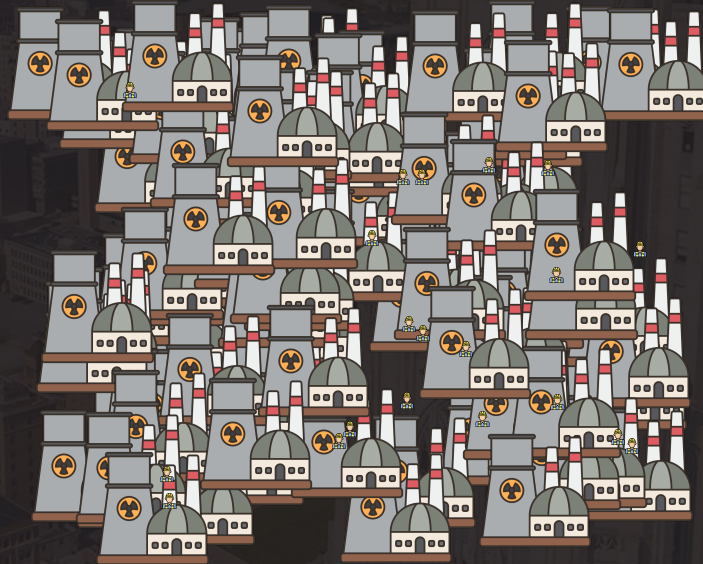
Formally Verified Autonomous Hybrid Control

Dane A. Sabo
dane.sabo@pitt.edu

Dr. Daniel G. Cole
dgcole@pitt.edu

University of Pittsburgh

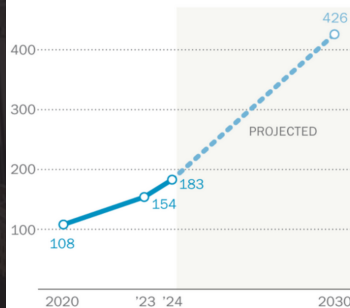
December 7, 2025



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

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)



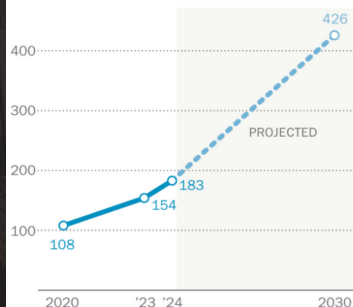
Source: Pew Research Center, Data from IEA

How much baseload power increase is this?

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

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!

Nuclear reactors are operated with prescriptive handbooks and legacy control technologies



Building a fleet of new reactors with current requirements will be an incredible staffing challenge

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



For one Small Modular Reactor (SMR)...

Building a fleet of new reactors with current requirements will be an incredible staffing challenge

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

24/7 operations require ~ 6 shifts:



For one Small Modular Reactor (SMR)...



12 SROs



12 ROs



24 licensed operators per reactor

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

Building a fleet of new reactors with current requirements will be an incredible staffing challenge

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

24/7 operations require ~ 6 shifts:



For one Small Modular Reactor (SMR)...



12 SROs

12 ROs

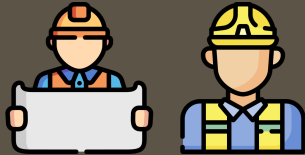
24 licensed operators per reactor

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

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

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 formally verified



Human reactor operators have key limitations that limit nuclear buildout

Humans cannot meet labor demand



Procedures are not formally 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:

- $K_{\text{eff}} < 0.99$
- 0% power
- $T_{\text{avg}} < 200^{\circ}\text{F}$

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.

Westinghouse Technology Systems Manual, Section 19.0 - Plant Operations

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:

- $K_{\text{eff}} < 0.99$
- 0% power
- $T_{\text{avg}} < 200^{\circ}\text{F}$

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.

FRET Specification

INITIAL_CONDITIONS shall satisfy:

mode = MODE_5

$k_{\text{eff}} < 0.99$

power = 0

$t_{\text{avg}} < 200$

...

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 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.

FRET Specification

INITIAL_CONDITIONS shall satisfy:

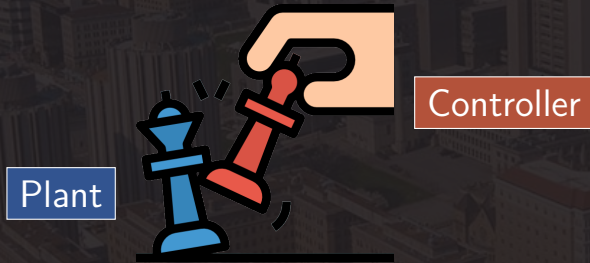
```
mode = MODE_5
k_eff < 0.99
power = 0
t_avg < 200
...
```

LTL Formula

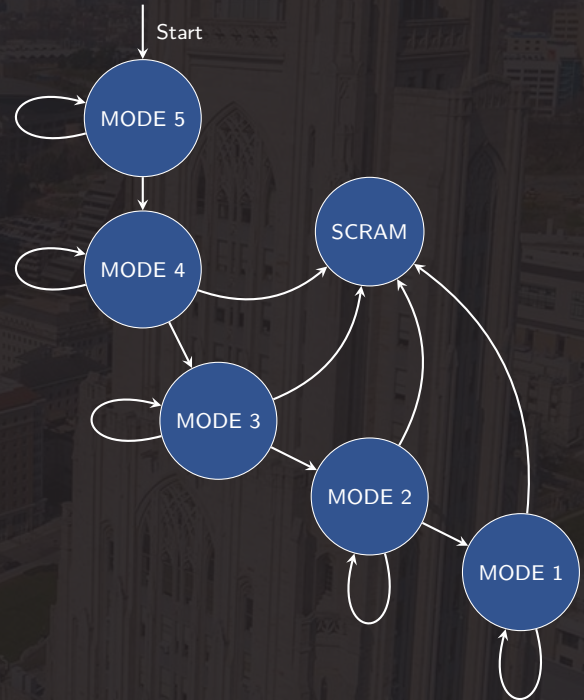
```
□ (initial → (
    mode_5_active ∧
    k_eff_subcritical ∧
    zero_power ∧
    temp_safe ∧
    ...))
```



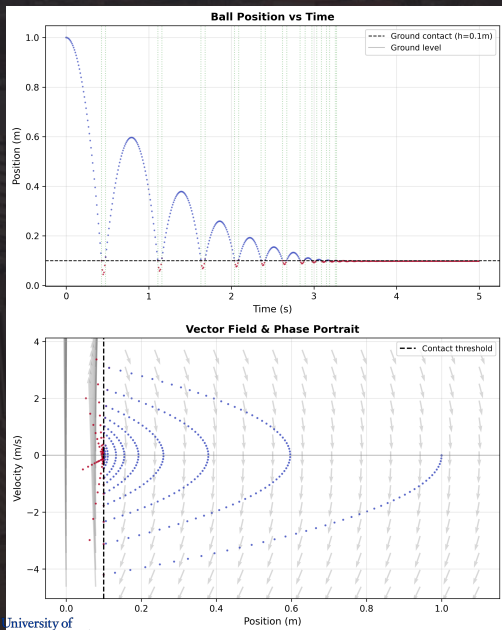
Second, we will use reactive synthesis to convert the logical formulae to generate discrete automata



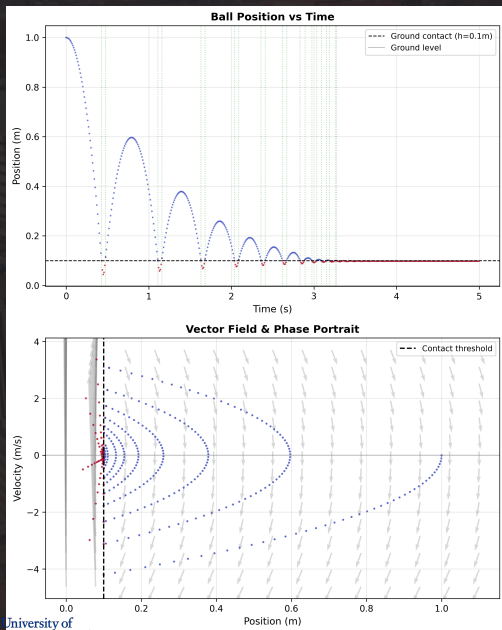
Second, we will use reactive synthesis to convert the logical formulae to generate discrete automata



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



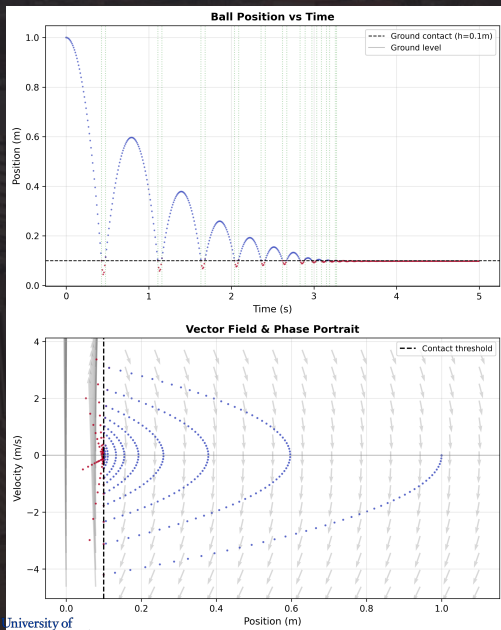
Finally, we will build continuous controllers to move between discrete states



Key Challenge

Verify continuous control behavior across discrete mode transitions

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



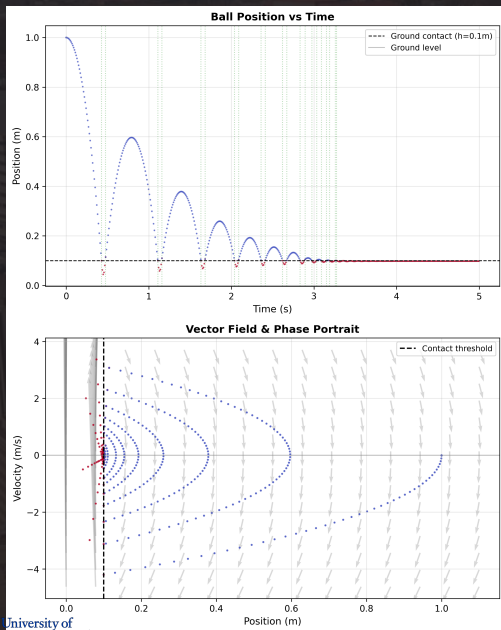
Key Challenge

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

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

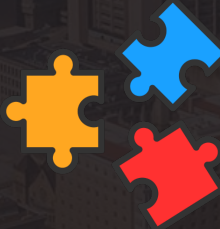
Success will be measured through Technology Readiness Level advancement

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

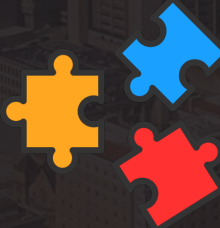
Success will be measured through Technology Readiness Level advancement

Why TRLs?

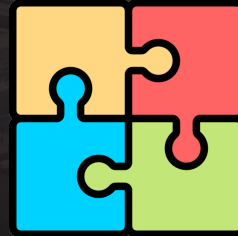
Bridge gap between proof-of-concept and deployment

Measure both rigor and feasibility

TRL 3
Components



TRL 4
Integration



Current: TRL 2-3

Target: TRL 5

Success will be measured through Technology Readiness Level advancement

Why TRLs?

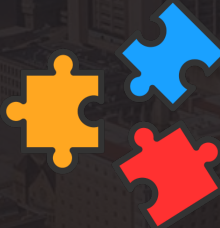
Bridge gap between proof-of-concept and deployment

Measure both rigor and feasibility

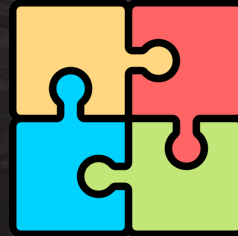
Current: TRL 2-3

Target: TRL 5

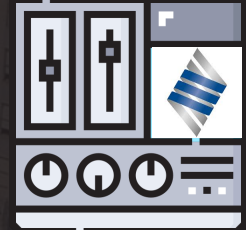
TRL 3
Components



TRL 4
Integration



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

Broader Impact: Multi-billion dollar O&M cost reduction

The Economic Opportunity

Datacenter electricity demand projected to reach **1,050 TWh/year** by 2030

If supplied by nuclear power:

$$\begin{aligned}\text{Total annual cost} &= 1,050 \text{ TWh/yr} \times \$88.24/\text{MWh} \\ &= \mathbf{\$92.7 \text{ billion/year}}\end{aligned}$$

Broader Impact: Multi-billion dollar O&M cost reduction

The Economic Opportunity

Datacenter electricity demand projected to reach **1,050 TWh/year** by 2030

If supplied by nuclear power:

$$\begin{aligned}\text{Total annual cost} &= 1,050 \text{ TWh/yr} \times \$88.24/\text{MWh} \\ &= \mathbf{\$92.7 \text{ billion/year}}\end{aligned}$$

O&M represents 23-30% of LCOE:

$$\begin{aligned}\text{O\&M costs} &= \$92.7\text{B} \times 0.23\text{-}0.30 \\ &= \mathbf{\$21\text{-}28 \text{ billion/year}}\end{aligned}$$

Broader Impact: Multi-billion dollar O&M cost reduction

The Economic Opportunity

Datacenter electricity demand projected to reach **1,050 TWh/year** by 2030

If supplied by nuclear power:

$$\begin{aligned}\text{Total annual cost} &= 1,050 \text{ TWh/yr} \times \$88.24/\text{MWh} \\ &= \mathbf{\$92.7 \text{ billion/year}}\end{aligned}$$

O&M represents 23-30% of LCOE:

$$\begin{aligned}\text{O\&M costs} &= \$92.7\text{B} \times 0.23\text{-}0.30 \\ &= \mathbf{\$21\text{-}28 \text{ billion/year}}\end{aligned}$$

Beyond nuclear: A generalizable framework for safety-critical autonomy

Why Nuclear First?

- Highest regulatory requirements
- Most safety-critical domain
- Procedures already documented
- Establishes regulatory pathway

Future Applications

- Chemical process control
- Aerospace systems
- Autonomous transportation
- Critical infrastructure

Translate procedures → Synthesize logic → Verify behavior
Applicable to any hybrid system with documented operational requirements

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

