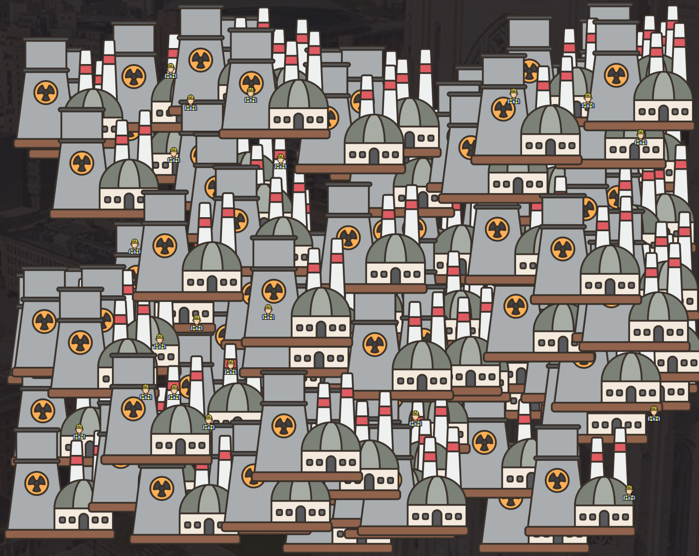
Formally Verified Autonomous Hybrid Control



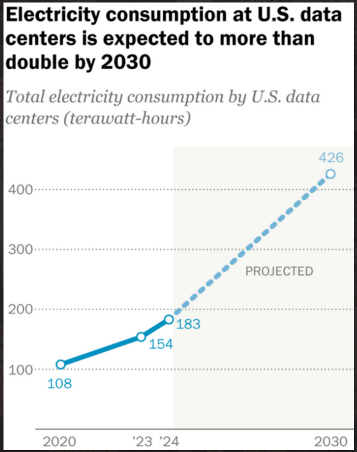
Dane A. Sabo
dane.sabo@pitt.edu

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

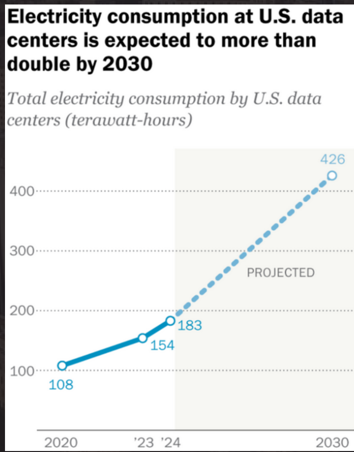


Source: Pew Research Center, Data from IEA

How much baseload power increase is this?

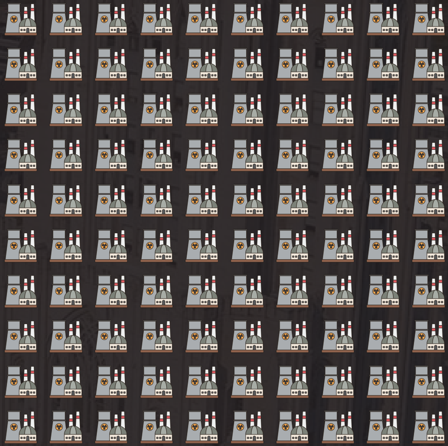
University of Pittsburgh
Cyber Energy Center

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



Source: Pew Research Center, Data from IEA

How much baseload power increase is this?



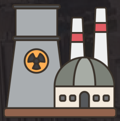
30 gigawatts!

Nuclear reactors are operated with prescriptive handbooks and legacy control technologies

University of Pittsburgh
Cyber Energy Center

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?



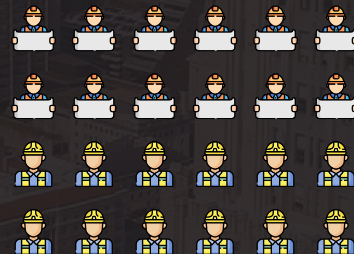
For one Small Modular Reactor (SMR)...

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?

For one Small Modular Reactor (SMR)...

24/7 operations require ~6 shifts:



12 SROs

12 ROs

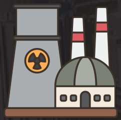
24 licensed operators per reactor

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

University of Pittsburgh
Cyber Energy Center

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)...

24/7 operations require ∼6 shifts:

12 SROs

12 ROs

24 licensed operators per reactor

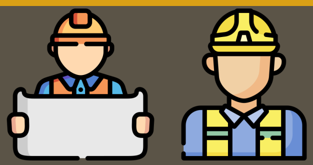
To meet demand we require 2,400 new licensed operators!

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

University of Pittsburgh
Cyber Energy Center

Human reactor operators have key limitations that limit nuclear buildout

Humans cannot meet labor demand



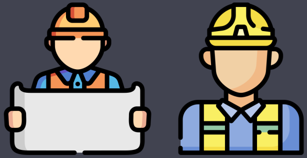
Human reactor operators have key limitations that limit nuclear buildout

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

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:

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

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.

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_{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.

Westinghouse Technology Systems Manual, Section 19.0 - Plant Operations

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
   - $T_{avg} < 200°F$
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

FRET Specification

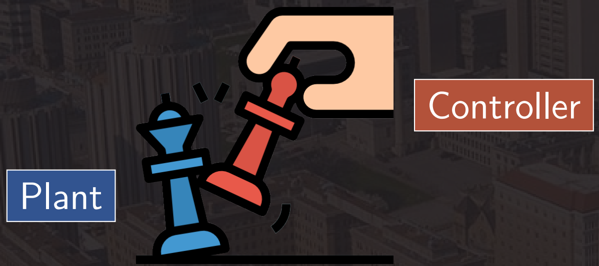
```
INITIAL_CONDITIONS shall satisfy:
      mode = MODE_5
      k_eff < 0.99
      power = 0
      t_avg < 200
      ...
```

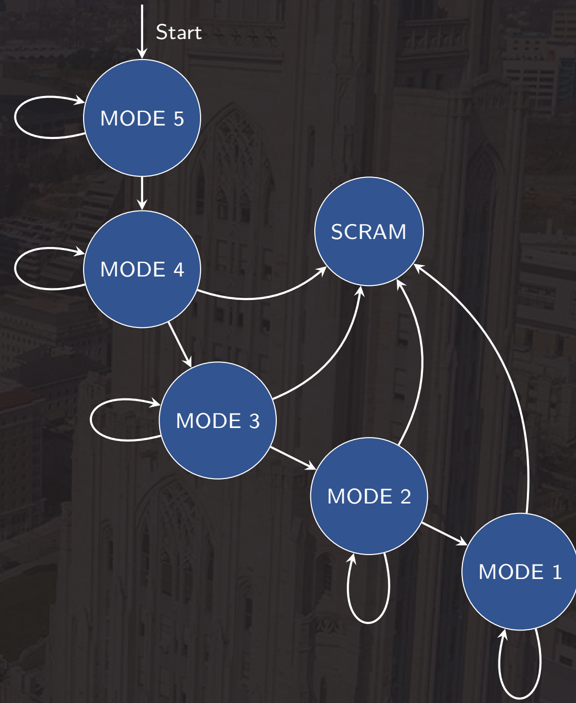
LTL Formula

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

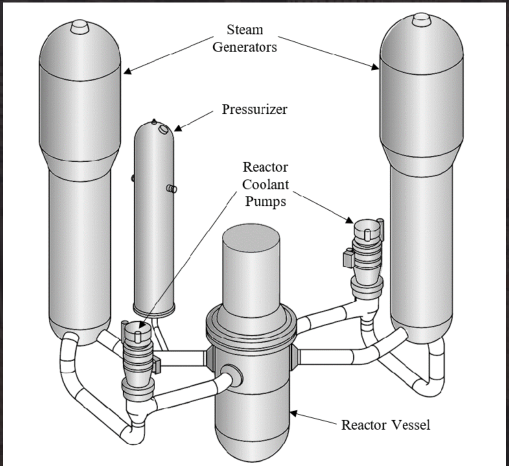
University of Pittsburgh
Cyber Energy Center

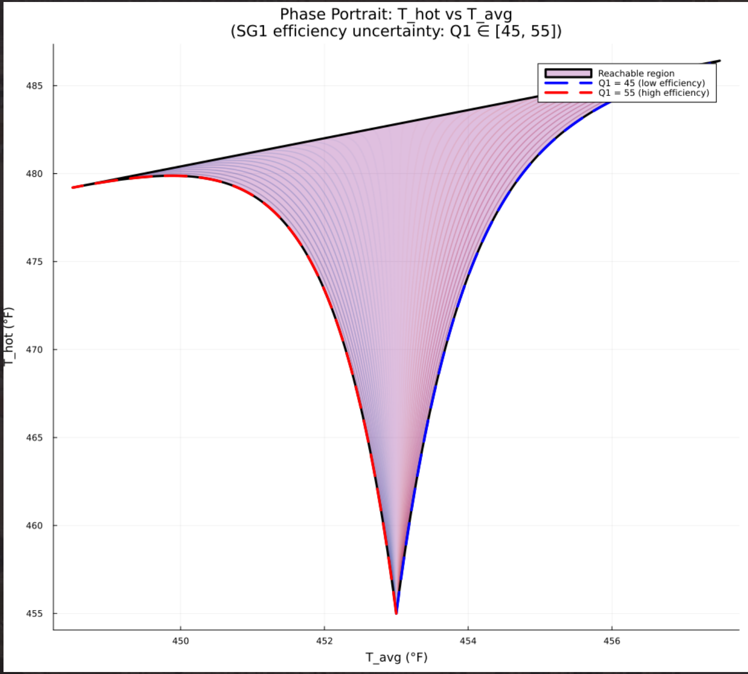
Second, we will use reactive synthesis to convert the logical formulae to generate discrete automata





Finally, we will build continuous controllers with formal methods to ensure transitions between modes



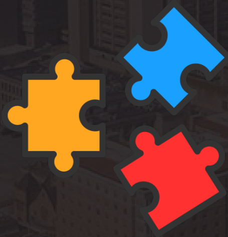


Success will be measured through Technology Readiness Level (TRL) advancement

TRL Goal

Current: TRL 2-3
Target: TRL 5

TRL 3
Components



Success will be measured through Technology Readiness Level (TRL) advancement

TRL 3
Components

TRL 4
Integration

TRL Goal

Current: TRL 2-3
Target: TRL 5

Success will be measured through Technology Readiness Level (TRL) advancement

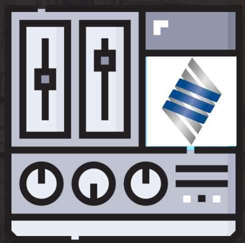
TRL Goal

Current: TRL 2-3
Target: TRL 5

TRL 3
Components

TRL 4
Integration

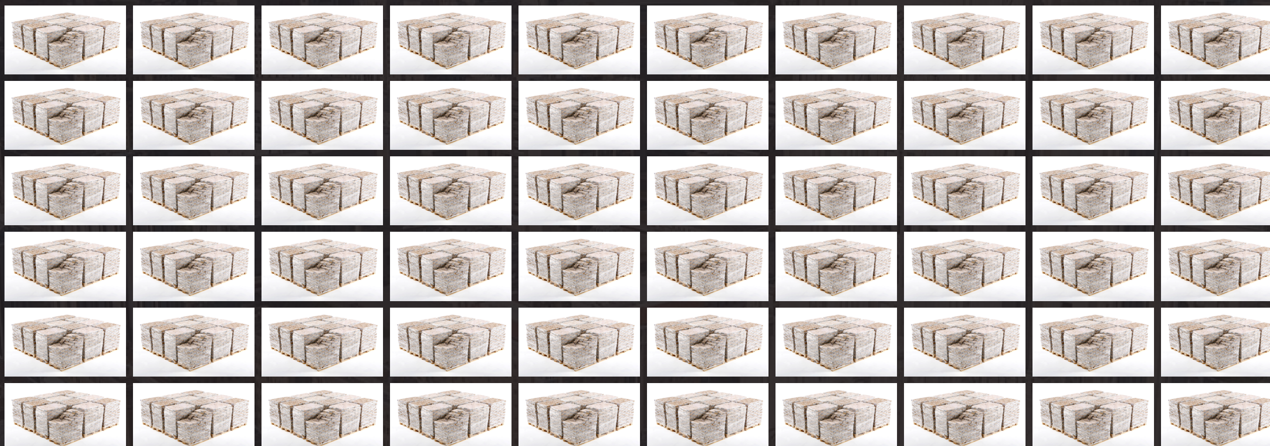
TRL 5
Hardware



Reducing operations costs for new nuclear power is a billion dollar problem

University of Pittsburgh
Cyber Energy Center

Reducing operations costs for new nuclear power is a billion dollar problem



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

Four primary risks are identified with clear mitigation and contingency plans

1. Computational Tractability of Synthesis

University of Pittsburgh
Cyber Energy Center

Four primary risks are identified with clear mitigation and contingency plans

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

University of Pittsburgh
Cyber Energy Center

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

University of Pittsburgh
Cyber Energy Center