Characterizing Nuclear Cybersecurity Using AI/ML

Advanced Sensors and Instrumentation (ASI) Annual Program Webinar

November 4, 2024

Acting Branch Chief: Sergiu Basturescu

U.S. Nuclear Regulatory Commission

Research Overview

Research into digital instrumentation and control systems, electrical engineering and cybersecurity.

Instrumentation & Control

Research on safety hazard identification for digital control systems. Provide technical research to support licensing decisions for modern digital controls and instrumentation.

Electrical Engineering

Research associated with modern battery technologies, operating plants not connected to the electrical grid, and enabling safe operation during long-term (60 yr+) plant operation.

Cybersecurity

Research to ensure the protection of critical digital assets associated with safety, security, and emergency preparedness functions at nuclear facilities.

Project Overview

Future Focused Research

Characterizing Nuclear Cybersecurity States with AI/ML

NRC Researchers:
Doug Eskins, Anya Kim, Kaitlyn Cottrell

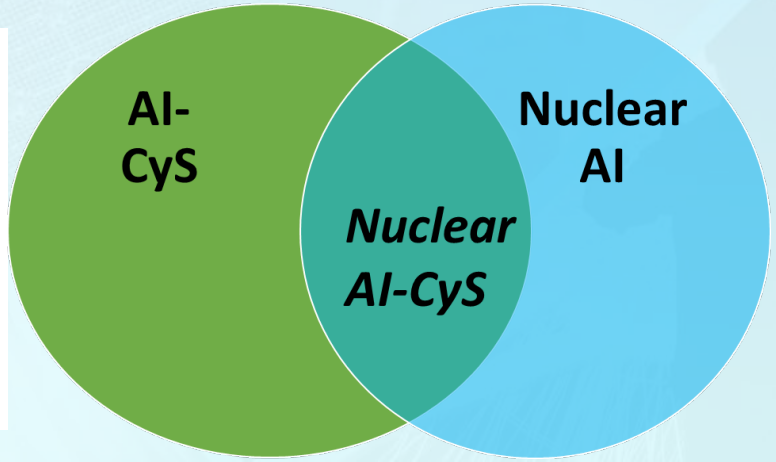
Regulatory Need: The NRC must prepare for potential use of AI/ML for licensee cybersecurity applications.

Project Goals

Develop Basic Knowledge of AI/ML Applications for Nuclear Cybersecurity

Prepare for Future Cybersecurity Regulatory Needs & Decision Making

Develop NRC Staff AI/ML Competencies



Project Start: Oct 2022 **Project Finish**: May 2024

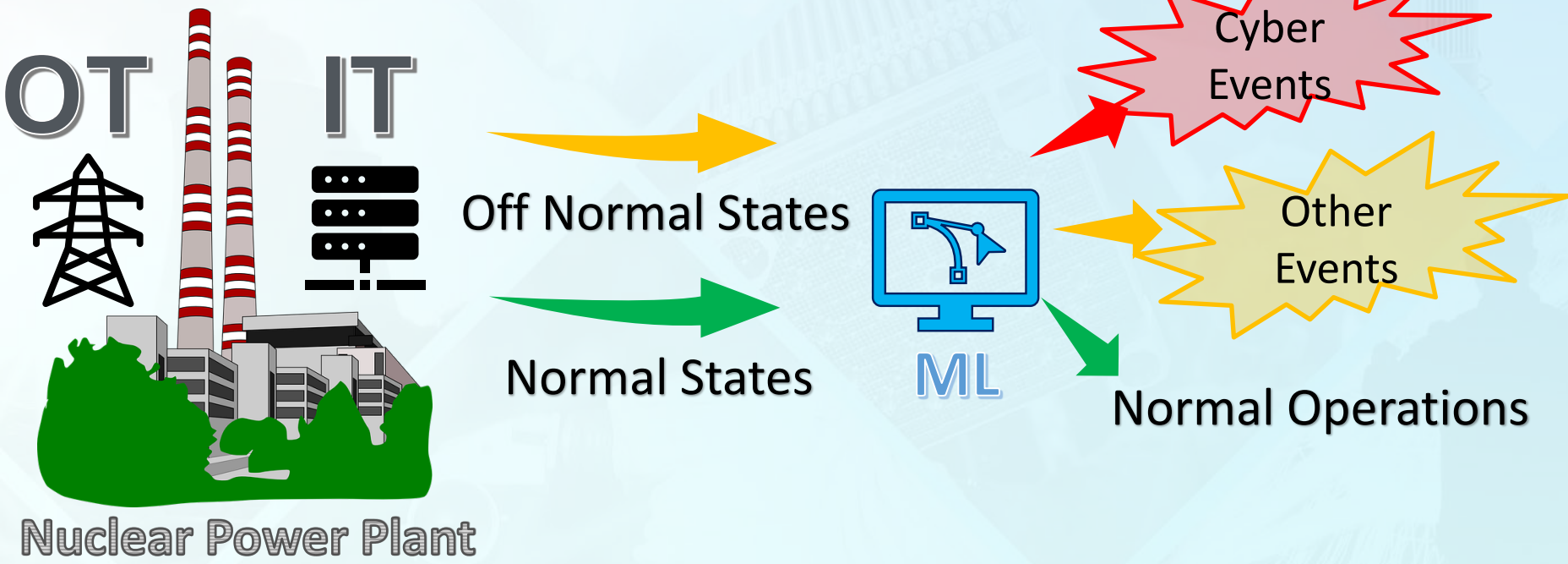
Project Overview

Identify Nuclear AI-CyS Use Case → Data Collection & Model Training → Performance Evaluation & Gap Analysis → Develop & Document Insights

OBJECTIVES

(1) Explore the use of AI/ML to **classify** nuclear cybersecurity states

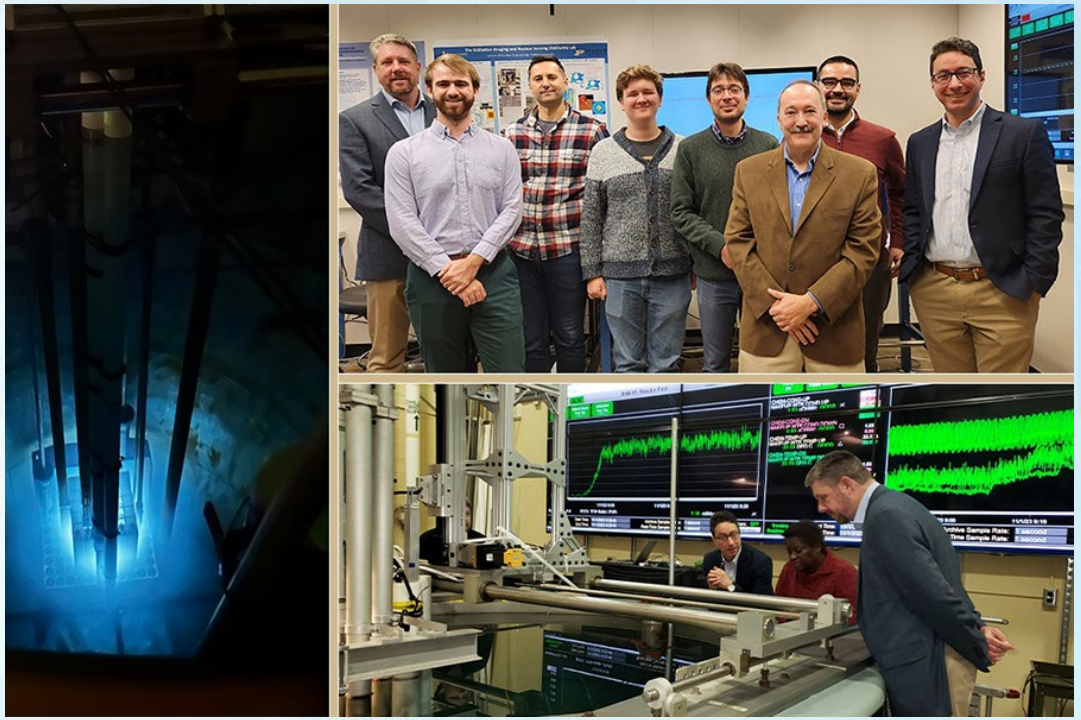
(2) Develop insights for **assessment** of nuclear AI-CyS



Project Team

NRC

- Doug Eskins (nuclear, M&S*)
- Kaitlyn Cottrell (AI/ML)
- Anya Kim (cybersecurity)



https://engineering.purdue.edu/NE/news/2023/us-nrc-visits-the-school-of-nuclear-engineering

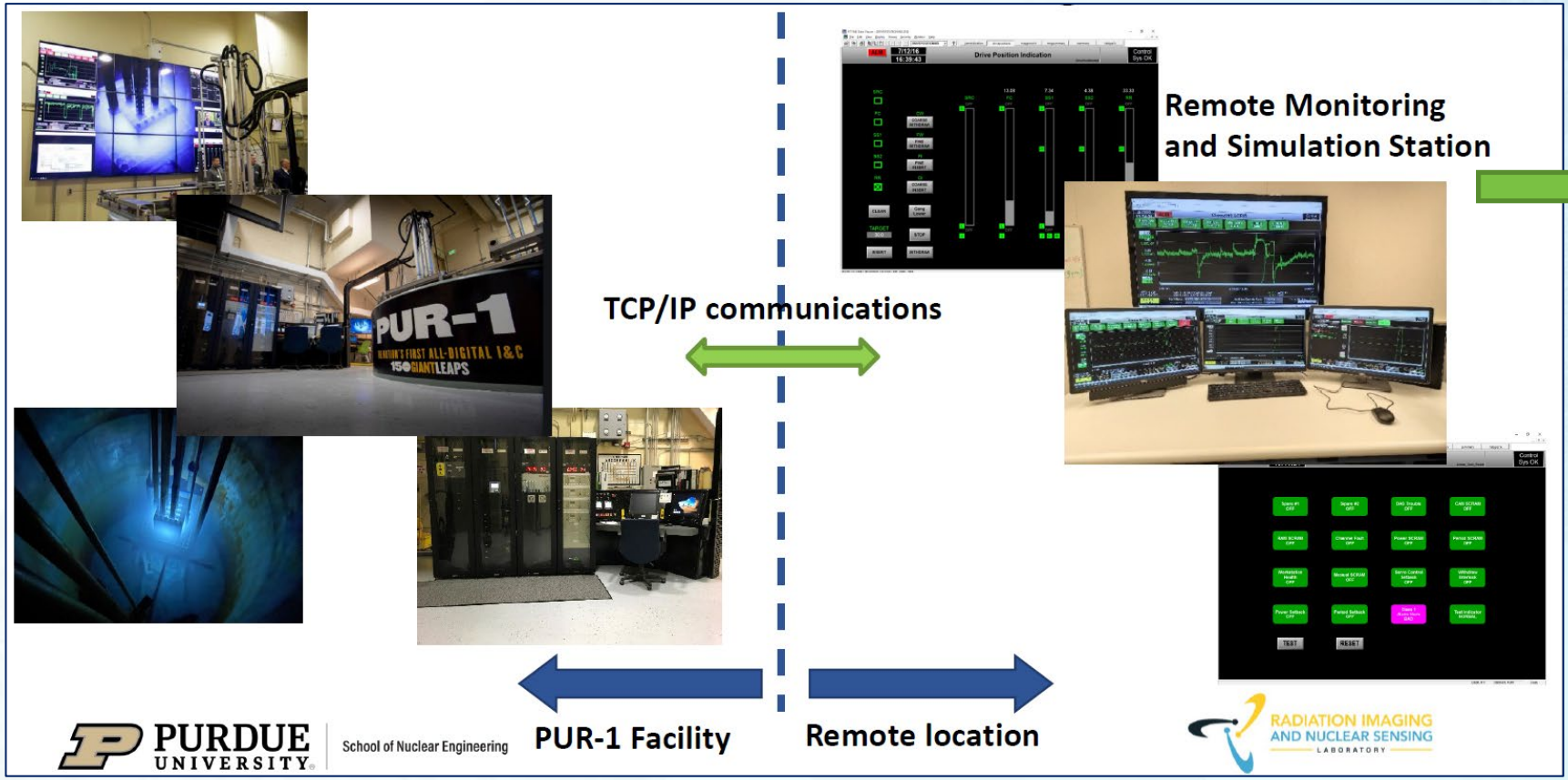
Purdue University

- Prof. Stylianos Chatzidakis (Dir Nuclear Engineering Radiation Lab)
- 5 graduate students (nuclear, AI, M&S)

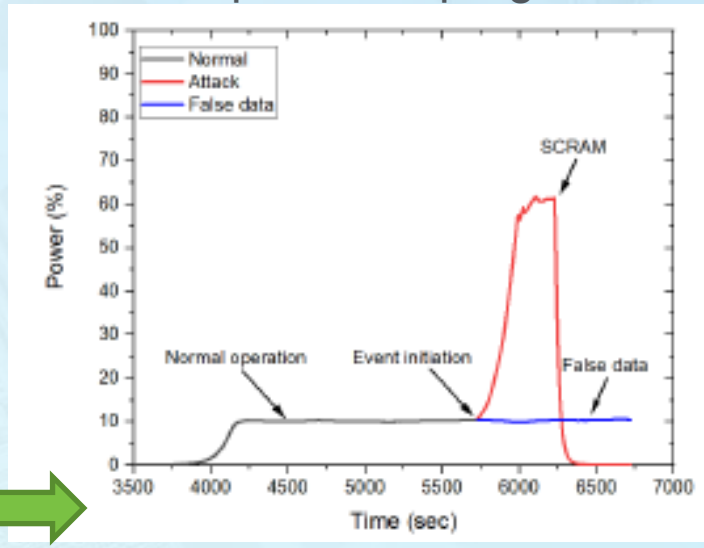
* Modeling and Simulation

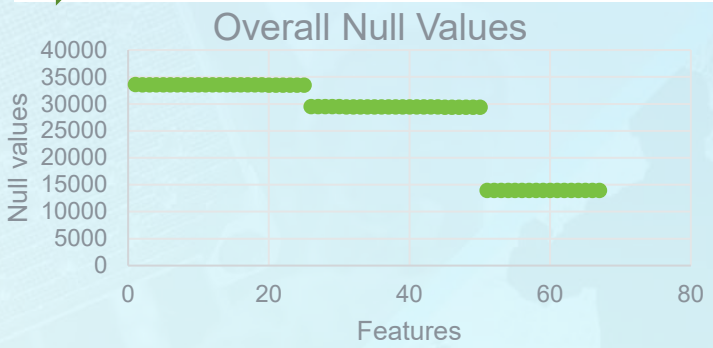
Challenges and Insights

- Real data
- Algorithm performance
- Data Management
- Data artifacts
- Robustness
- Explainability

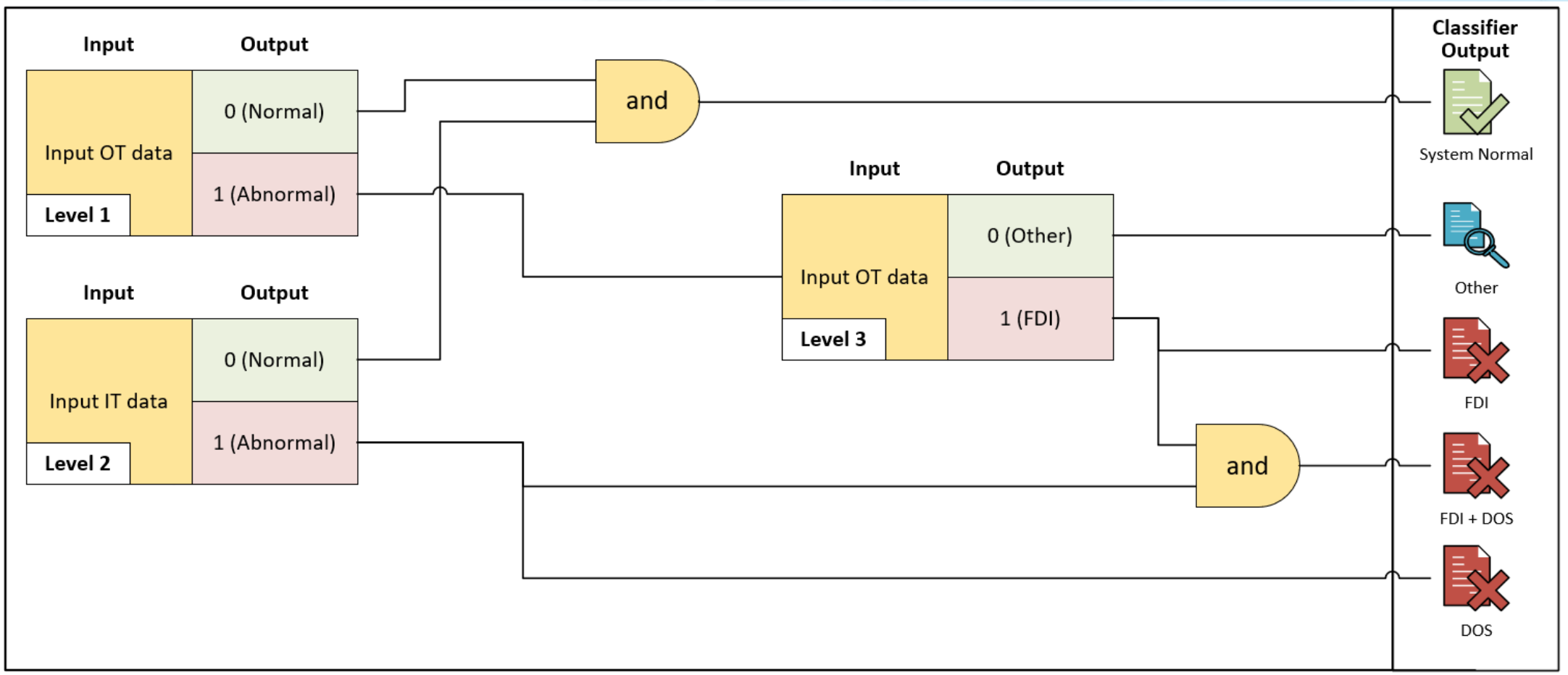


Example event progression





Composite Classifier



Reports

- Research Plan Development (TLR-RES/DE-2024-003a), ML23040A169
- Identification of a Representative Use Case (TLR-RES/DE-2024-003b), ML23062A349
- Identification of AI-ML Technology (TLR-RES/DE-2024-003c), ML23102A182
- Use Case Implementation (TLR-RES/DE-2024-003d), ML24052A002
- Performance Evaluation and Gap Analysis (TLR-RES/DE-2024-003e), ML24193A007
- **Final Report:** Characterizing Nuclear Cybersecurity States using AI-ML (TLR-RES/DE-2024-003), ML24193A008

What's Next?

Future Work concerning

- Collecting the right data
- Managing change
- Understanding the vulnerabilities/ attack vectors introduced by AI
- Understanding the threat of attackers using AI
- Integration with humans
- Trusting AI
- Impact on NRC regulations and guidance

Christopher Cook
Branch Chief
Instrumentation, Controls, and Electrical Engineering Branch
Office of Nuclear Regulatory Research
United States Nuclear Regulatory Commission
Email: Christopher.Cook@nrc.gov

Sergiu Basturescu
Acting Branch Chief
Instrumentation, Controls, and Electrical Engineering Branch
Office of Nuclear Regulatory Research
United States Nuclear Regulatory Commission
Email: Sergiu.Basturescu@nrc.gov

Doug Eskins
Senior Computer Engineer
Instrumentation, Controls, and Electrical Engineering Branch
Office of Nuclear Regulatory Research
United States Nuclear Regulatory Commission
Email: Doug.Eskins@nrc.gov

Thank You