ADVANCED REACTOR SAFEGUARDS & SECURITY

SMR-THREAT

Enabling Threat Hunting for Small Modular Reactors

PRESENTED BY

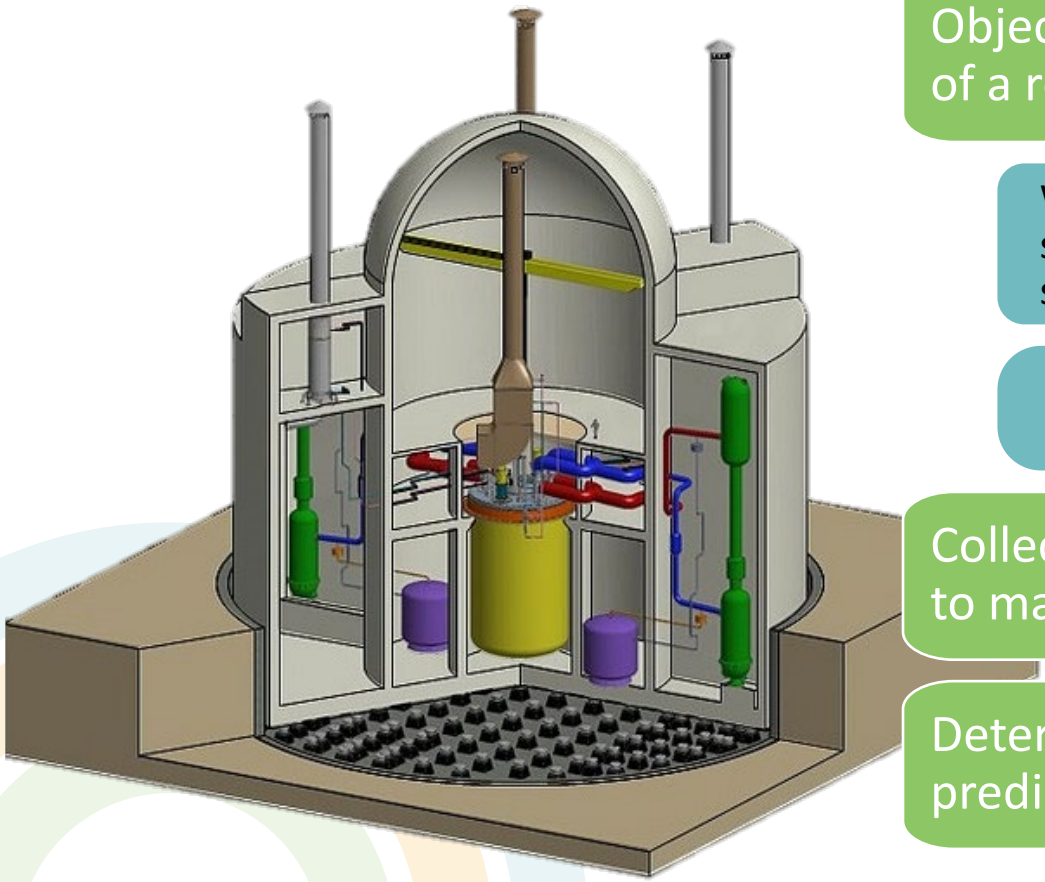
Glenn A. Fink, PhD, CISSP

15 April 2025

Savannah River National Laboratory® | U.S. DEPARTMENT OF ENERGY

SRNL-STI-2025-00229

Overview of SMR-THREAT



Objective: Predict the safety, security, and safeguards (3S) state of a remotely deployed SMR solely from the cyber data.

We define *cyber data* as the machine status and control data of the system passed across a digital network among operators, controllers, sensors, and effectors.

Primarily operational technology (OT) data over TCP/IP, but possibly other formats

Collect cyber data from an SMR surrogate and study the ability to make accurate assessments to preserve 3S stability.

Determine design constraints and recommendations that make prediction possible and reliable.

The SMR Surrogate facility

- Mobile facility to down-blend nuclear materials of concern for nonproliferation
- Safety, Security, and Safeguards concerns
- Used here as a simple surrogate for an SMR

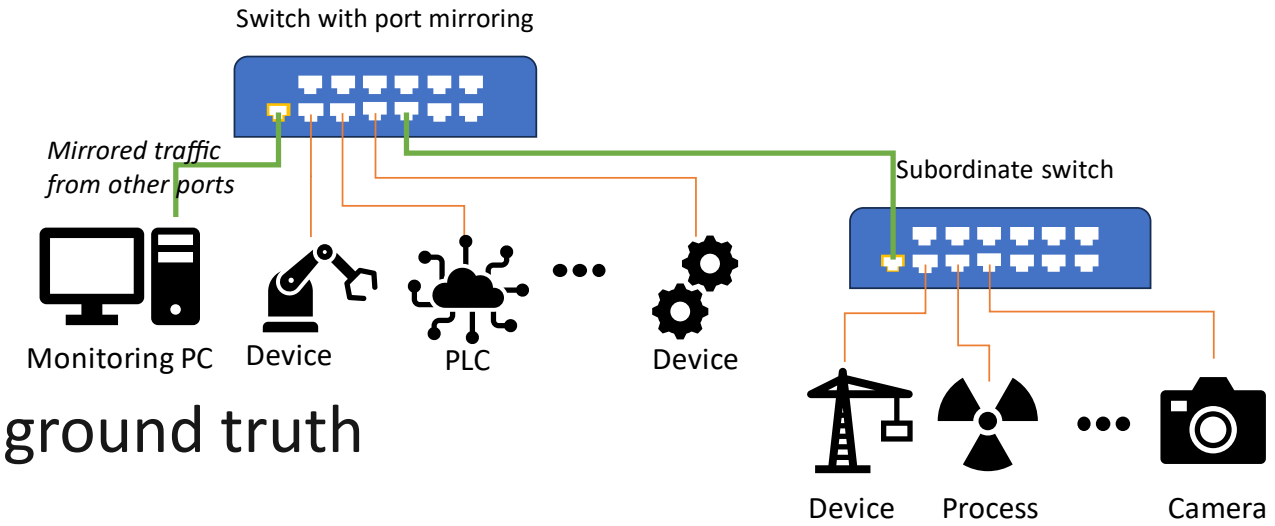
Load NMOC → Melt & Stir → Cool → Discharge → Package

Motivation and Research Questions

- Motivation: Early detection and diagnosis of faults and cyber attacks in A/SMRs
- Research Questions:
  - Can the 3S state of the system be estimated solely from the TCP/IP data on the OT networks?
  - Can a state estimation be interpreted earlier than an operator can react to system status?
  - How interpretable is a state anomaly found in network data for diagnosis?

Methodology

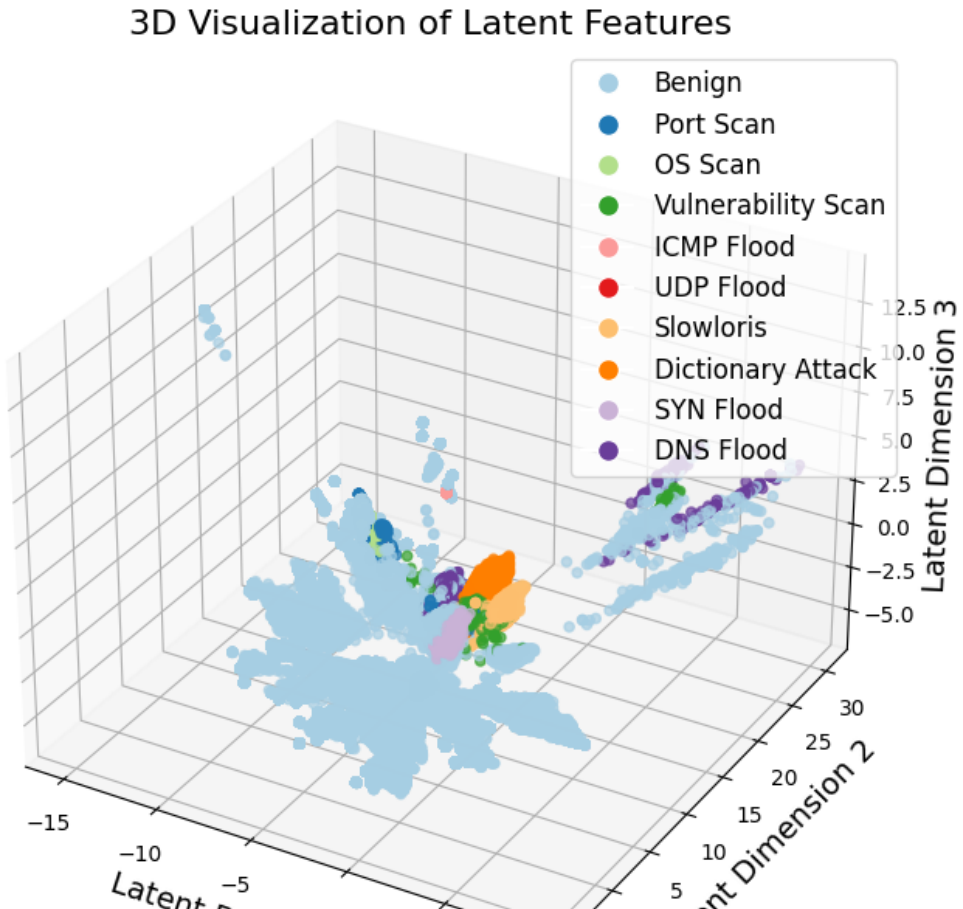
- Instrumented the surrogate system to enable data collection from a single point through port aggregation and mirroring
- Collected data through several complete operations
  - TCP/IP OT, IT, and video data
  - Operator manually entered logs
- Analyzed connectivity



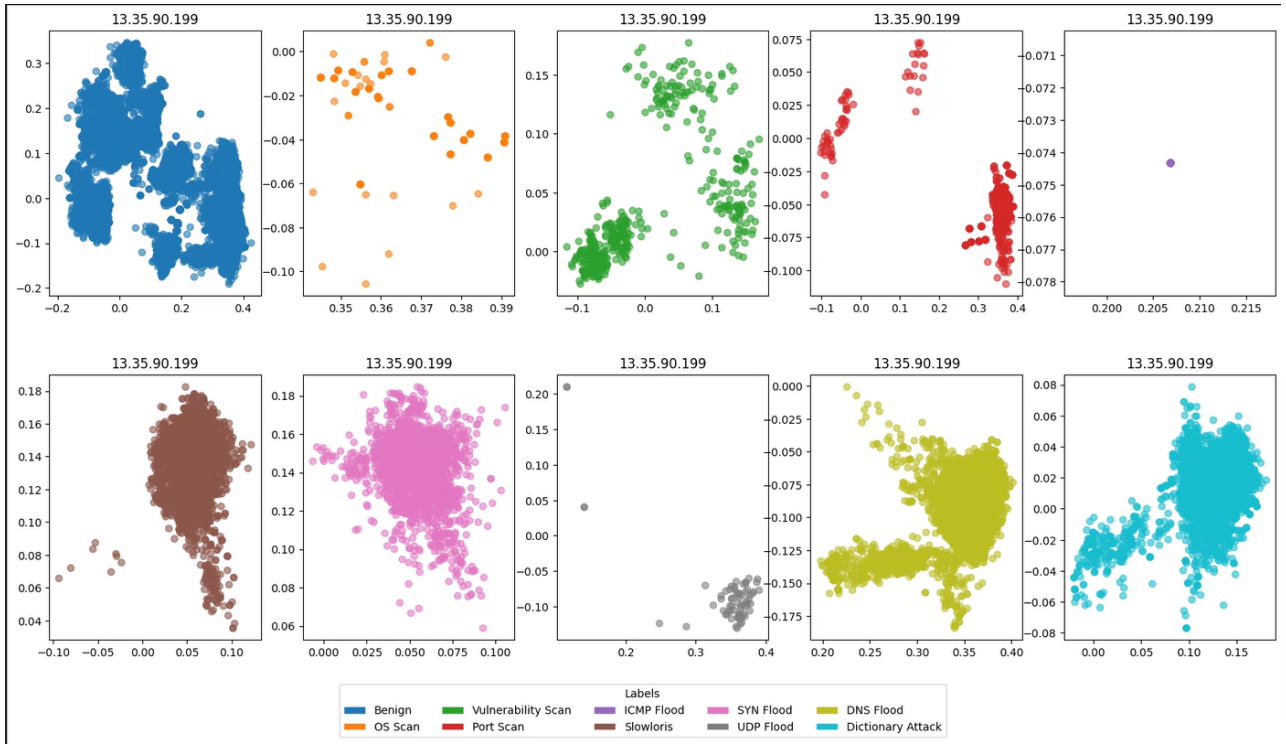
- Also using a separate data set with ground truth
  - ACI IoT intrusion data set
  - This is because of operational security issues the project faces

Results (ACI IoT data)

Embeddings show distinction of benign and malicious data



Malicious data types show clear modalities



Conclusion and Future Work

- Latent space state analysis can be accomplished through embeddings of OT TCP/IP data.
- Work continues in FY25 to
  - Process and plot actual surrogate data (overcoming administrative restrictions on data usage)
  - Interpret the differences shown between benign and malicious data and determine whether they are significant or spurious
  - Obtain more OT data from the surrogate and the wider SRS site (including labeled anomaly conditions)
  - Identify connections between cyber anomalies and events of concern in OT systems to draw conclusions about what is possible for SMRs