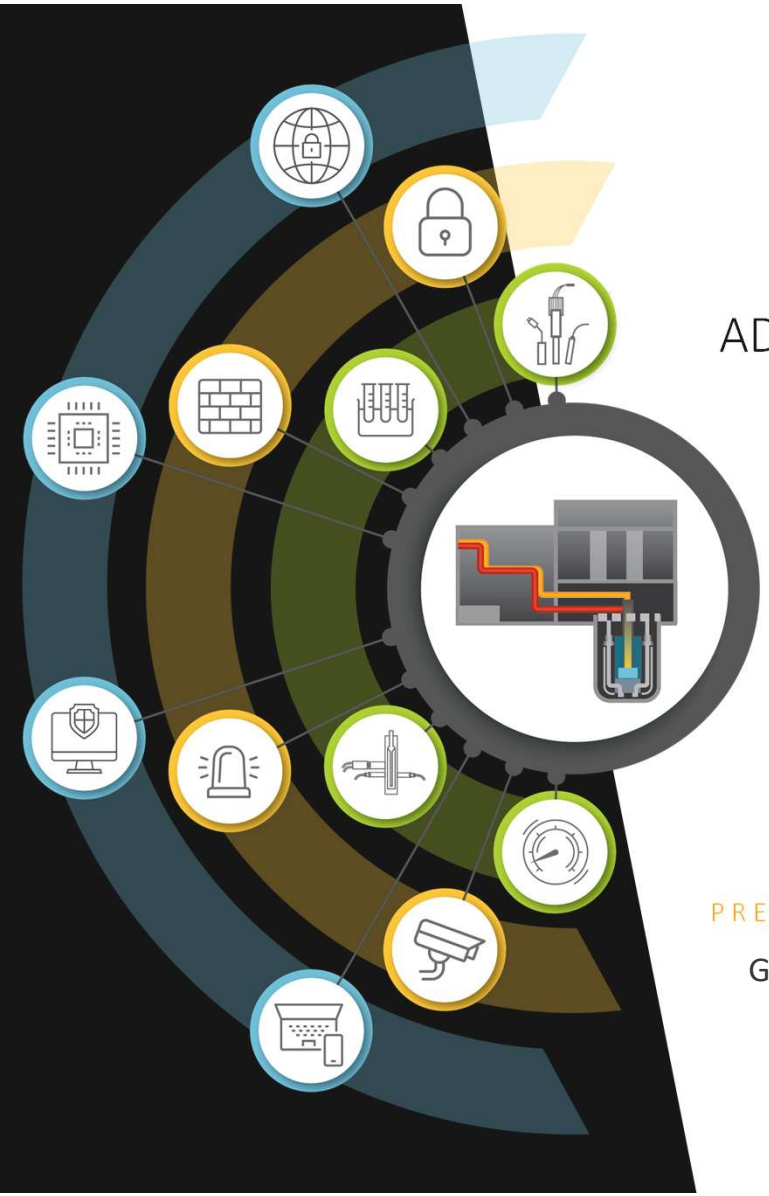


ADVANCED REACTOR SAFEGUARDS & SECURITY

SMR-THREAT 2.0

Enabling Threat Hunting for Small Modular Reactors

PRESENTED BY

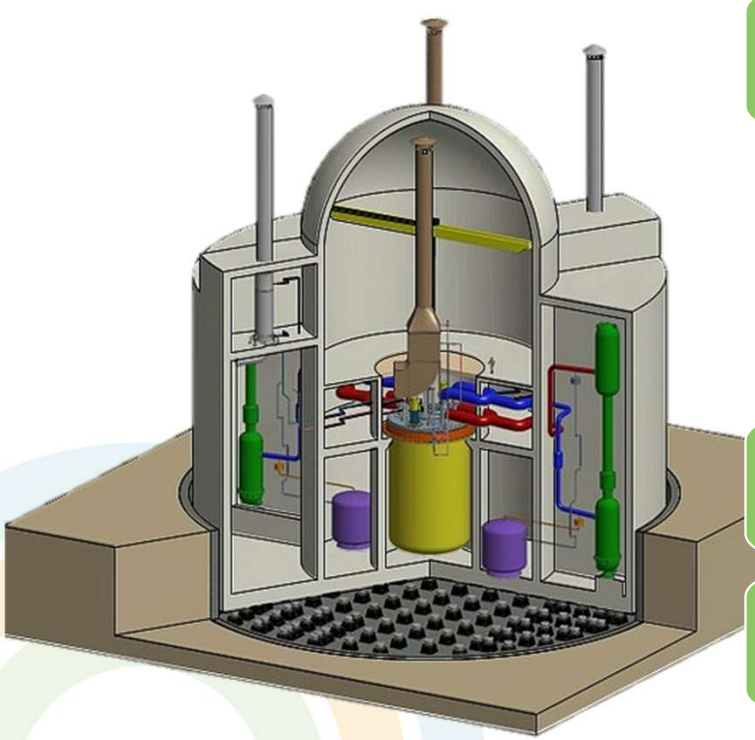
Glenn A. Fink, PhD, CISSP

27 April 2026

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

SRNL-STI-2026-00230

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, typically common industrial protocol (CIP), modbus, or dnp3 and other formats

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

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

Research Questions

- Q: Can the 3S state of the system be estimated solely from the TCP/IP data on the OT networks?
  - A: Yes, but not well. Cross-correlation with historian, OOB, and other sources gives a fuller picture.
- Q: Can a state estimation be interpreted earlier than an operator can react to system status?
  - A: Probably
- Q: How interpretable is a state anomaly found in network data for diagnosis?
  - A: Not good on its own but, combined with other data, quite interpretable.

Data sources

SRNL Melter

3 PLCs, ~40 devices

PCAP, ~20 sensors, and out-of-band data collection

Real physics; No attacks

Operation COYOTE (synthetic)

Hundreds of devices, simplified sodium test loop built from docs

PCAP, Zeek, Suricata, EVTX, 109 sensors, 9 OOB

Simulated; 110-day Volt Typhoon attack

SFR Test Loop? Or not?

More complex than COYOTE but less control

PCAP, Zeek, >110 sensors, OOB possible

Real physics; No attacks

Sensitivity issues

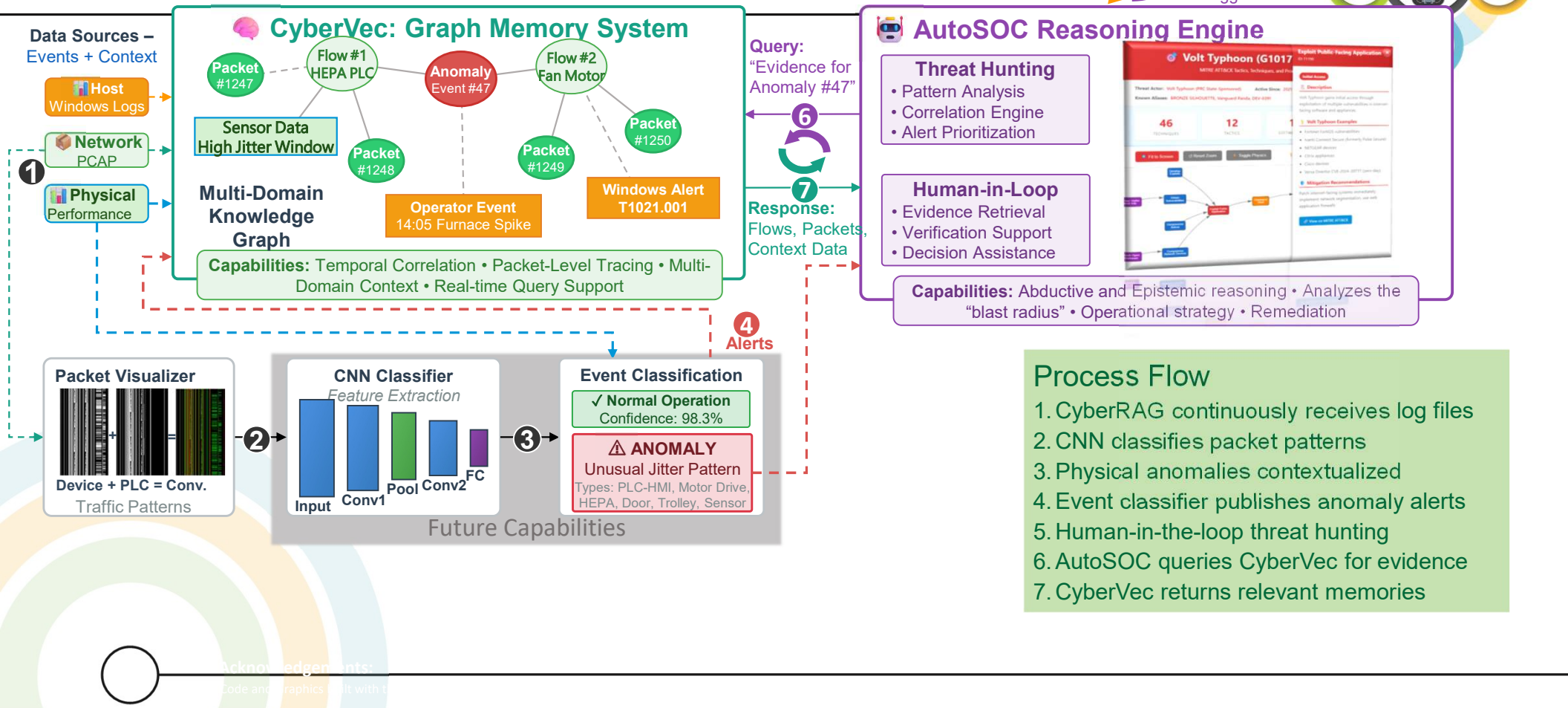
Savannah River National Laboratory®

COYOTE Dataset: Types & Amounts of Data

- The COYOTE dataset is a 7.2-GB, multi-stream, cross-layer cyber–physical benchmark designed to support research on detecting long-dwell APT activity in fictitious reactor OT environments.
- It includes seven primary data categories, each with its own structure, purpose, and volume.
  1. Attack Timeline (0.1 MB)
  2. OOB physical sensor data (0.9 GB)
  3. Historian data archive for 142 process tags including one with falsified data (6.0 GB)
  4. Windows event logs (EVTX) for the HMI and Historian, etc. (5.6 MB)
  5. Targeted packet captures for the OT system including normal baseline and simulated attack data (97 MB)
  6. Zeek data (network flows), generated from the packet captures
  7. Suricata alerts (247 MB)

- Attack data represents a complete fictitious 110-day Volt Typhoon attack on the reactor
- Approach: examine cross-layer activity to identify “events” that may indicate attack. At each stage, predict the attacker’s next moves.

AutoSOC: AI-Powered OT Threat Hunting Pipeline



Process Flow

1. CyberRAG continuously receives log files
2. CNN classifies packet patterns
3. Physical anomalies contextualized
4. Event classifier publishes anomaly alerts
5. Human-in-the-loop threat hunting
6. AutoSOC queries CyberVec for evidence
7. CyberVec returns relevant memories

Acknowledgements:
Code and graphics built with t

AutoSOC Demonstration

Accomplishments

- Coded initial AutoSOC reasoner and memory modules
- Built a synthetic demonstration data set, Operation COYOTE and drafted a paper on it
- Demonstrated AutoSOC to Southern Nuclear and others as potential follow-on work
- Submitting multiple proposals to explore aspects of the capability outside the ARSS mission space

Conclusion and Future Work

- Cross-layer analysis can more quickly identify, verify, and recommend resolution of 3S problems than single-layer approaches
- Mapping cyber data to telemetry events (changes, etc) is in progress
- Work continues to
  - Publish a paper on Operation COYOTE data set
  - Ingest test loop data with the Argonne team (overcoming sensitivity issues)
  - Connect with follow-on sponsors who can expand the work