

ADVANCED REACTOR SAFEGUARDS & SECURITY

Advanced Reactor Safeguards and Security: Application of Digital Twins

Nuclear Energy & Applications, UIUC

October 19-20, 2026

PRESENTED BY

Ben Cipiti

SAND2026-26108PE

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

A Changing Regulatory Landscape



Provided the Foundation for:

- Eliminating a set number of on-site responders
- Allowing for off-site response
- Changes to Secondary Alarm Station

2018

NRC Part 73 Limited Scope Rulemaking, SRM-SECY-18-0076

2019

NRC Part 53 rulemaking started due to NEIMA Act

2024

NRC Plans to Pull Part 73 Limited Scope Rulemaking into Part 53

2025

Trump Administration Executive Orders to Reinvigorate the U.S. Nuclear Industry

2026

DOE NE Authorization Pathway for Nuclear Facilities

NRC Part 53 completed

21 Nuclear Energy Directives and Policies related to the DOE NE authorization pathway for nuclear facilities, the main one being DOE-STD-1271-2025.

DOE NE Order 470.1, "Office of Nuclear Energy Safeguards and Security"

- Establishes high level guidance on safeguards and security
- Benefits include providing more flexibility for securing reactors and fuel cycle facilities.
- However, by itself, it does not provide detailed guidance to the nuclear industry.

Material Control and Accounting



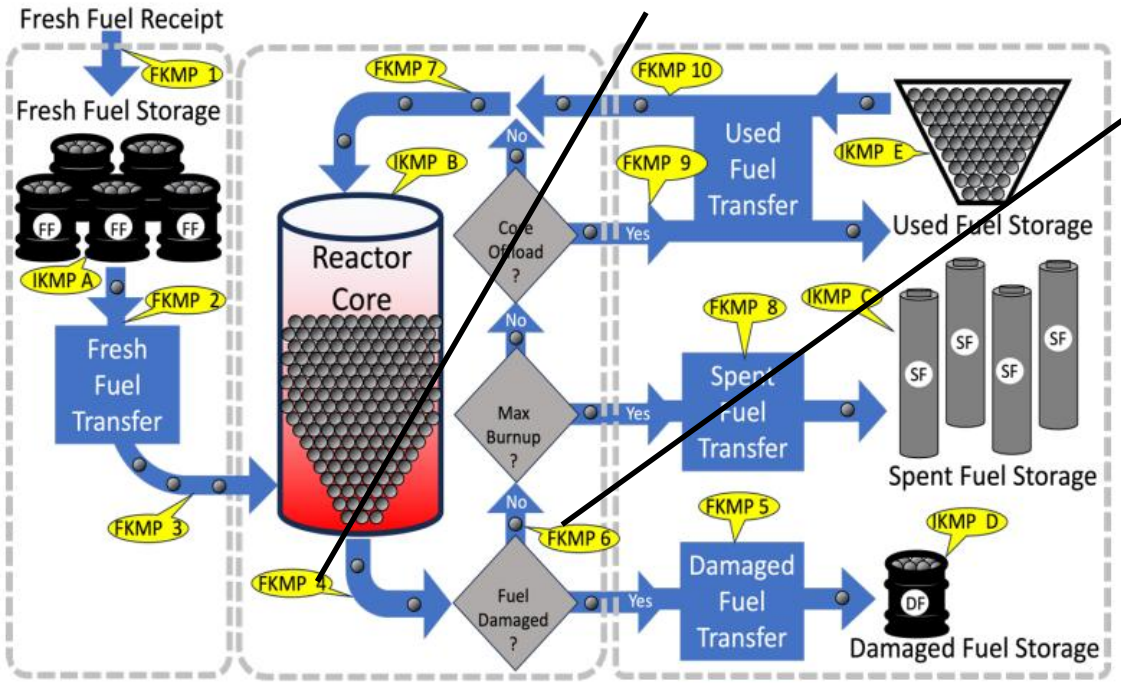
- From a domestic MC&A standpoint, most advanced reactors will follow the MC&A approach that existing large light water reactors follow: item accounting and use of burnup codes to declare inventories.
  - This will be true for any reactor that uses solid fuel assemblies or fuel elements.
  - But the codes may need to improve for some reactor types.
- Pebble Bed Reactors will have a slightly different approach due to the semi-bulk nature of the flowing pebbles.
- Liquid-fueled Molten Salt Reactors will also utilize a different approach due to the bulk (non-item) nature of the fuel.

MC&A for Pebble Bed Reactors

- From a domestic MC&A and international safeguards perspective, we only need to account for pebbles at the canister level (very dilute).
- From a process control standpoint, every spent pebble needs a burnup measurement (and this can be used to inform MC&A).
- From a physical security perspective we don't want to lose a spent pebble due to the threat of an RDD device.

Pebble Integrity Measurement to look for damaged fuel

Burnup Measurement (BUMS) for process control and actinide estimate



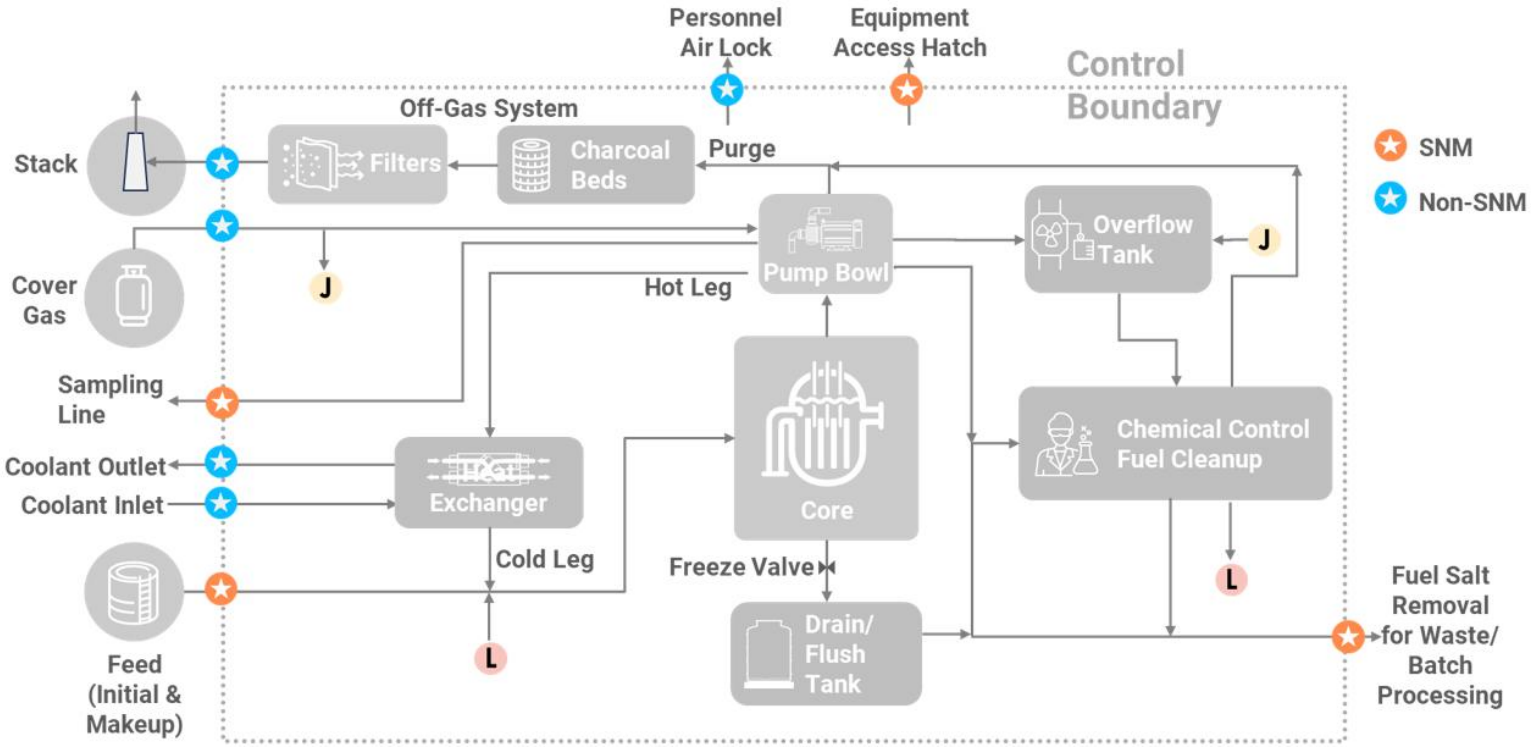
D. Kovacic et al. "Nuclear Material Control & Accounting for Pebble Bed Reactors," Oak Ridge National Laboratory, ORNL/SPR-2023/2988 (December 2023).

A Digital Twin may be used for material control and accounting. A digital twin of the reactor core may be used to keep track of pebble burnup and total actinide quantities, but note that it's impossible to predict pebble path through the reactor.

MC&A for Molten Salt Reactors

- Molten Salt Reactors have challenges with MC&A due to the difficulties of getting low uncertainty actinide total measurements in a large bulk reactor loop.
- MSRs may rely additionally on a control boundary approach where monitoring is used for key penetrations and access points to the reactor loop.

A Digital Twin also may be used for material control and accounting. It's likely that vendors will want to use sampling or on-line measurements to validate reactor models.



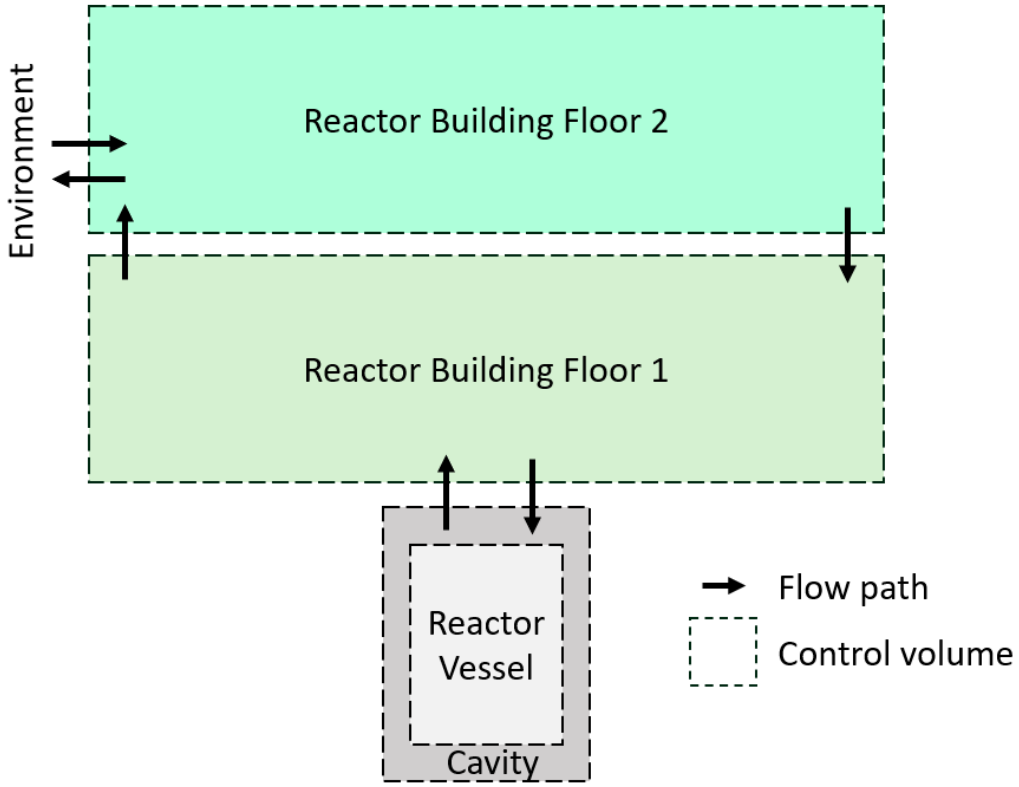
S. Chirayath et al. "Control Boundary Analysis for Liquid-Fueled Molten Salt Reactors," Oak Ridge National Laboratory, ORNL/SPR-2025/4221 (September 2025).

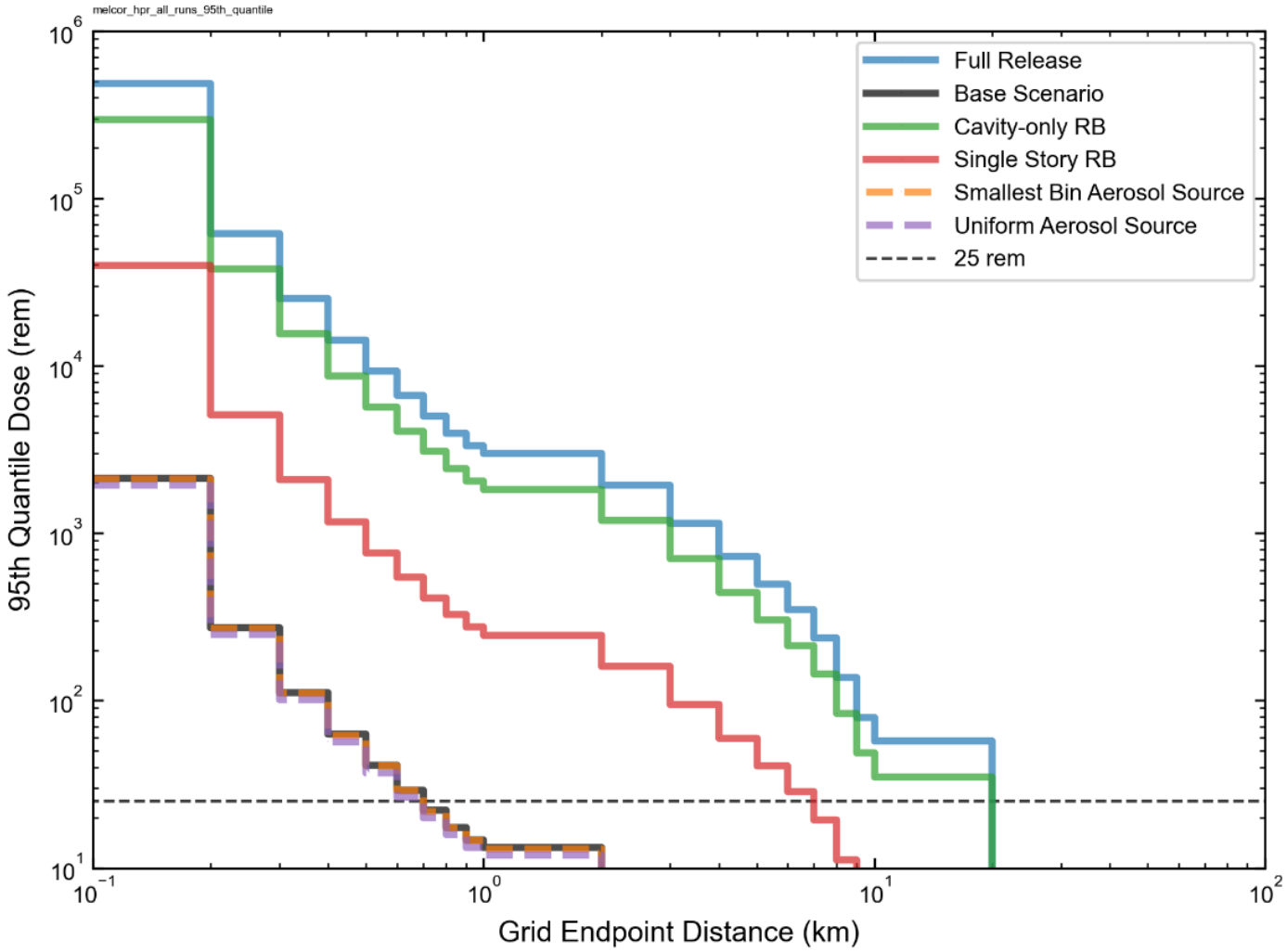
Consequence Analysis: Physical Protection and Cybersecurity Implications



- Based on the new Part 53 (and Part 57), if a reactor vendor (or other nuclear facility) can prove that the dose at the site boundary is <25 rem over 2 hours for a worst-case credible sabotage scenario, they may be alleviated from the need to respond to the Design Basis Threat (DBT).
- This has significant economic implications due to the cost of maintaining on-site responders or cost of contracting with off-site response.
- Our technical recommendation is to assume a DBT-type of attack with no mitigation (attackers will have a lot of time).
- "Credible" is the important word here—the vendor should perform the analysis to be bounded in reality using conservatism only where it makes sense.

Consequence Analysis Preview





C. Faucett et al. "Integrated Security-Safety Consequence Study of a Heat Pipe Reactor," Sandia National Laboratories, SAND2026-22860 (June 2026).

Consequence Analysis Implications



- If the vendor can prove <25 rem at the site boundary (through direct sabotage, indirect attack of safety systems, and cyber or cyber-physical attack), the PPS moves toward an order-compliance approach. The following recommendations follow this type of approach:
  - The reactor site should still have intrusion detection, access control, and material access areas.
  - Security staff should still be utilized for entry control and contraband detection.
  - On-site responders will not be required.
  - Cybersecurity controls may be greatly reduced with instead a focus on maintaining reactor operation, also traditional NRC rules which bar the use of wireless or remote operations for safety and important to safety systems may not apply.

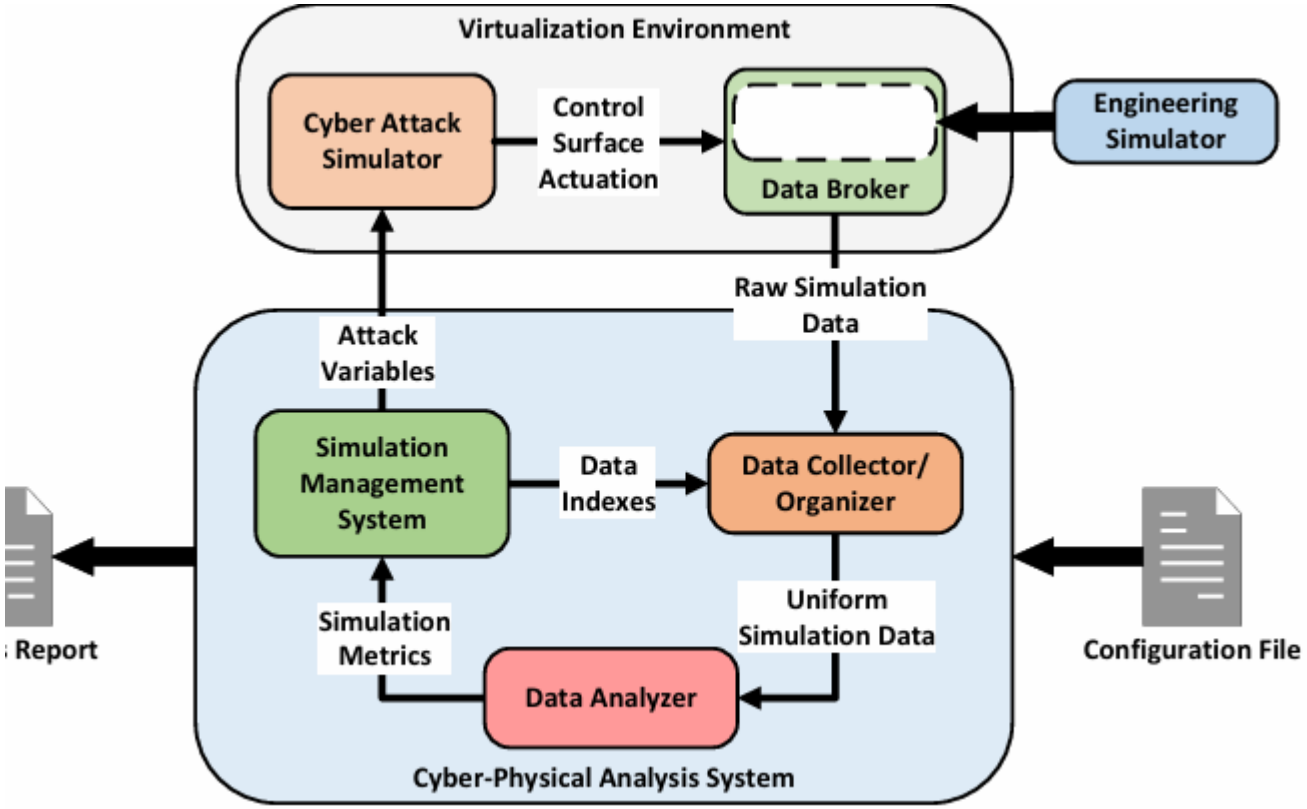
So What's This Have to do with Digital Twins?



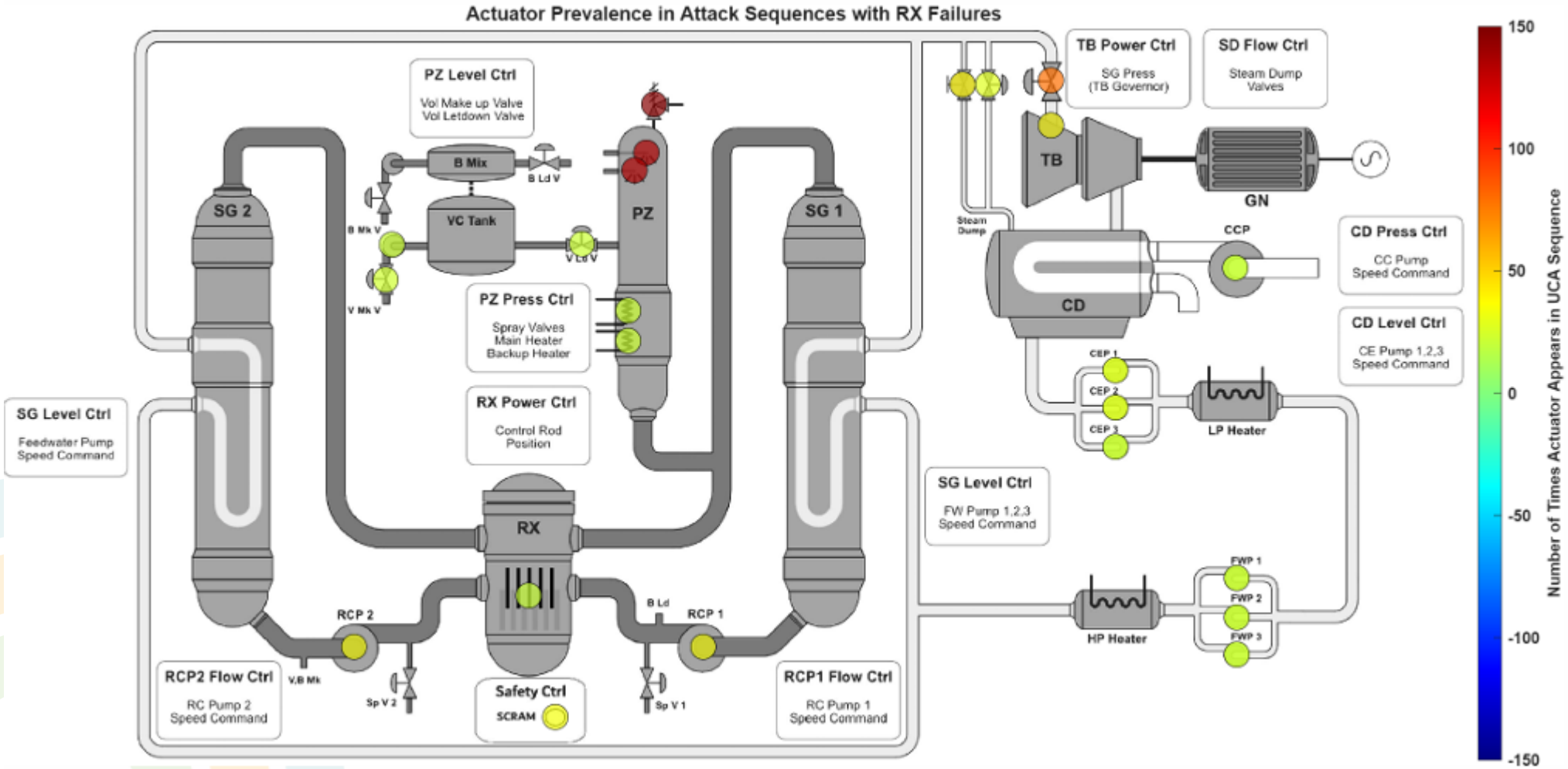
- There's really no need for a digital twin to help with physical security.
- A digital twin for cyber attacks could be interesting, but is it worth it?
  - For microreactors that can prove the <25 rem threshold, the number of critical digital assets is drastically reduced, so monitoring for cyber attack may not be needed. Cyber protections then fall back to NERC/FERC requirements and become more about keeping the plant on-line.
  - For reactors that can't or choose not to prove the <25 rem threshold, now cyber attacks are more of a concern for safety. A digital twin may be a way to actively monitor for cyber attack.

Overview of ARCADE

- ARCADE links to an engineering simulator (digital twin) to simulate a large range of unsafe control actions (UCAs).
- The purpose is to determine which systems are most critical and those for which compromise will not lead to a UCA.
- Ultimately this helps to optimize and reduce the number of cyber security controls.



Asherah Model Results

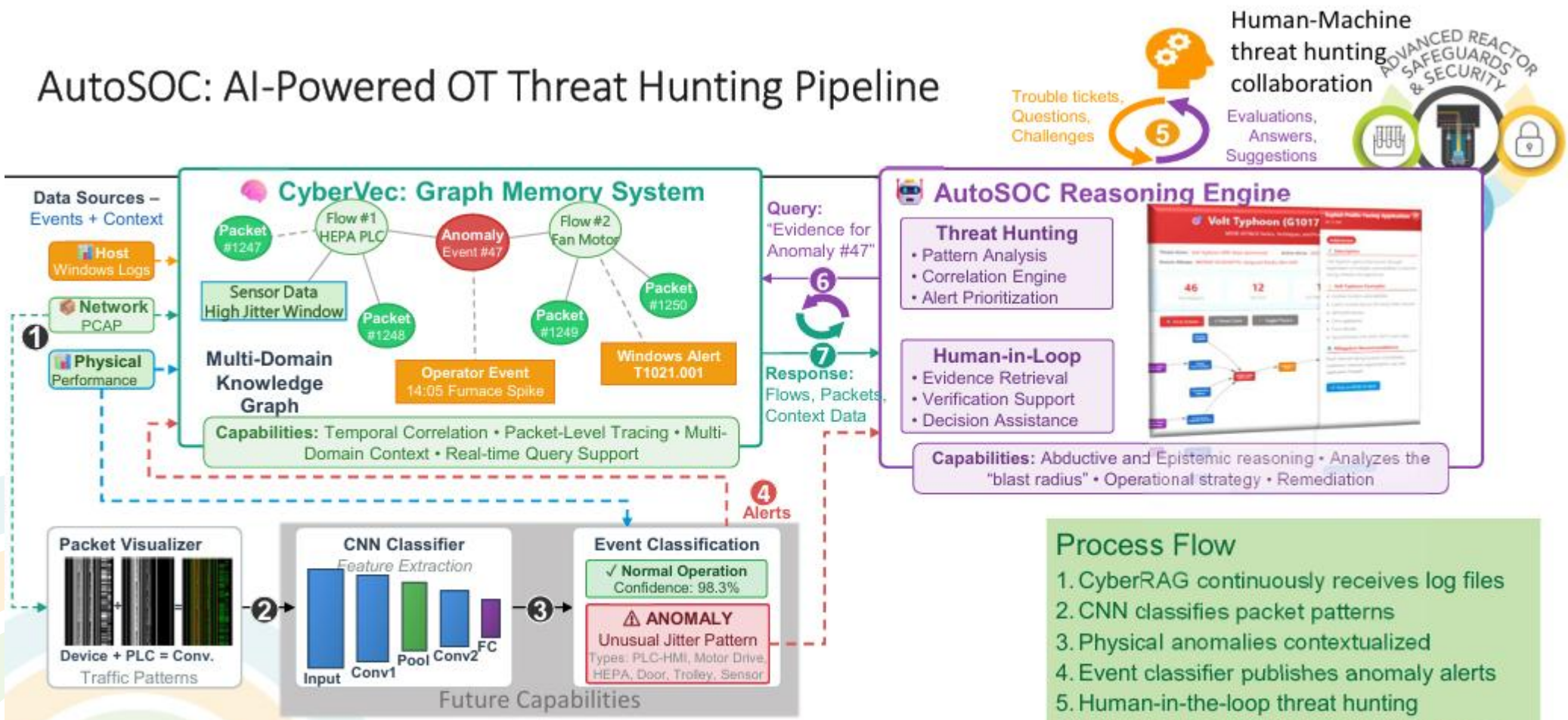


Overview of SMR-THREAT



- Objective: Predict the safety, security, and safeguards state of a remotely deployed SMR solely from cyber data.
  - Cyber data is the machine status and control data of the system passed across a digital network among operators, controllers, and senors.
  - Primarily operation technology (OT) data over TCP/IP (Transmission Control Protocol/Internet Protocol)
- Collect cyber data from an SMR or surrogate facility and study the ability to make accurate assessments to preserve 3S stability
- Determine design constraints and recommendations that make prediction possible and reliable

AutoSOC: Threat Hunting



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

Conclusions



- From a domestic MC&A perspective, digital twins may be used to report inventories and may have a larger role for the more exotic reactor designs like PBRs and MSRs.
  - Note that our program area does not look at International Safeguards, so there may be other applications in that space.
- Probably not a need for digital twins in the physical security space.
- There are various applications of digital twins for both cybersecurity design and monitoring after reactors are operating.

Thank You!

Open reports are posted to the program website:

https://energy.sandia.gov/arss

For additional information:

Ben Cipiti, National Technical Director (SNL) bbcipit@sandia.gov

Dan Warner, Federal Program Manager daniel.warner@nuclear.energy.gov