SAND2024-14890C

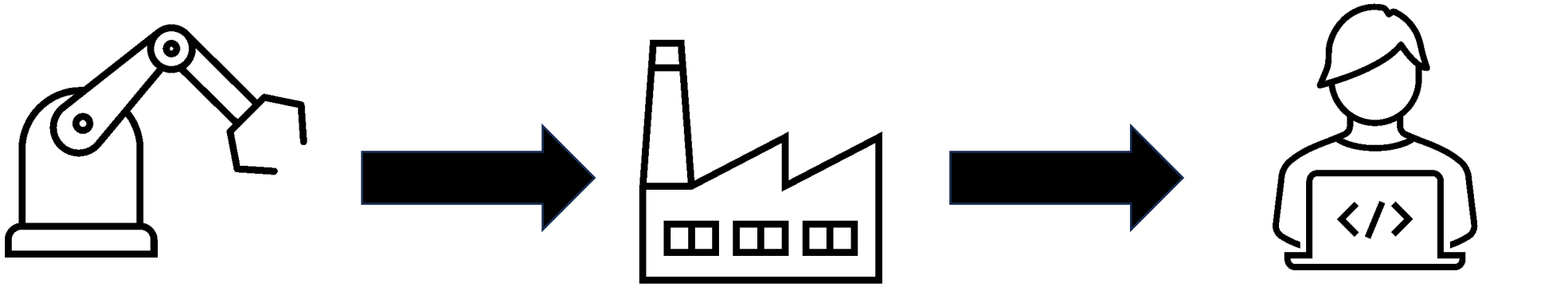
U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response

Development of a Cyber-Physical Model and Emulation of an Oil and Gas Compressor Station for Cybersecurity R&D

Lee Maccarone

2024 IEEE SR-CIST Workshop

Reactive cybersecurity R&D is not efficient



Novel OT Control Technologies

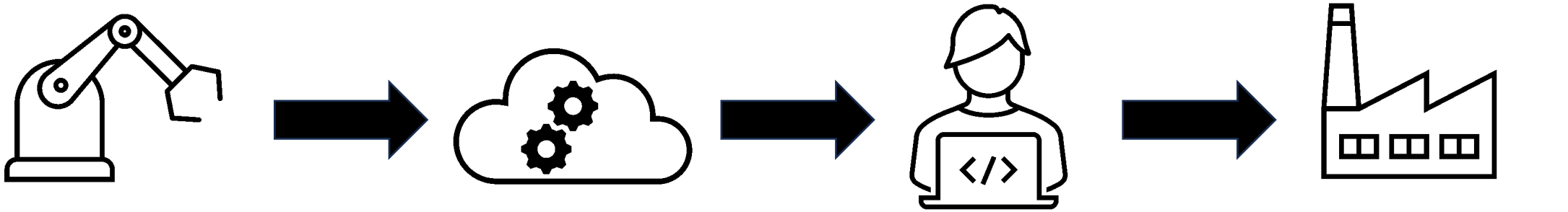
Industrial Deployment

OT Cybersecurity R&D

Need: High-Fidelity Simulation Data for OT Systems

- Development of novel OT regularly outpaces OT cybersecurity R&D
- OT security analysis should be consequence-focused and integrated with the design process
- OT security engineers need a platform to perform cyber-physical security analyses of their systems

Proposed Framework: Proactive Security R&D



Novel OT Control Technologies

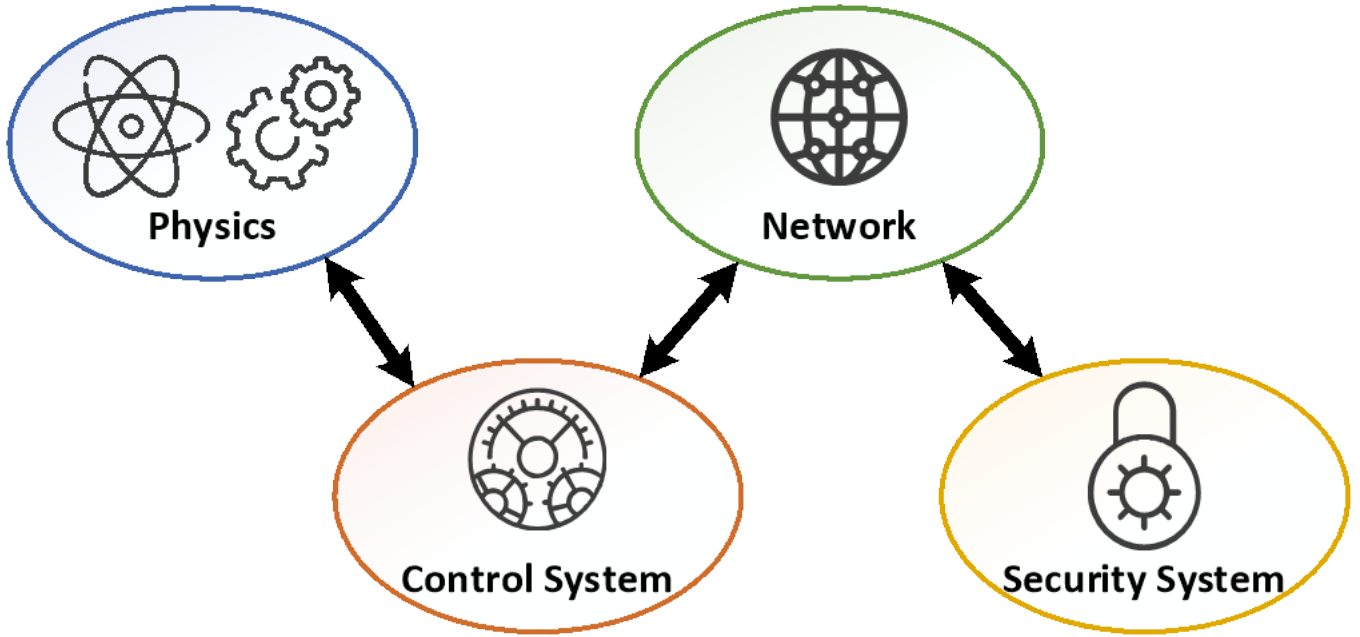
Testbed Deployment

OT Cybersecurity R&D

Industrial Deployment

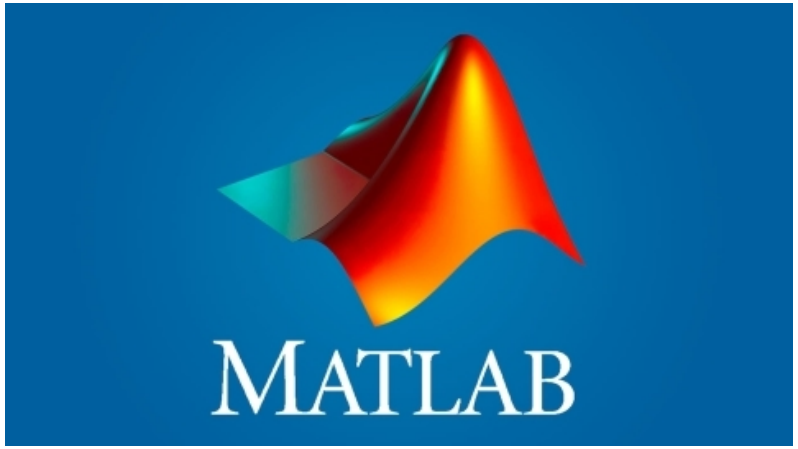
Approach: Fusion of Physics Simulation and OT Device Emulation

- Couple a high-fidelity physics simulation engine with emulated OT environment
- Perform real-time integration of physics data with emulation environment, simulating a realistic plant setting
- Derive security system events and unsafe control actions from simulated physical effects of cyberattacks



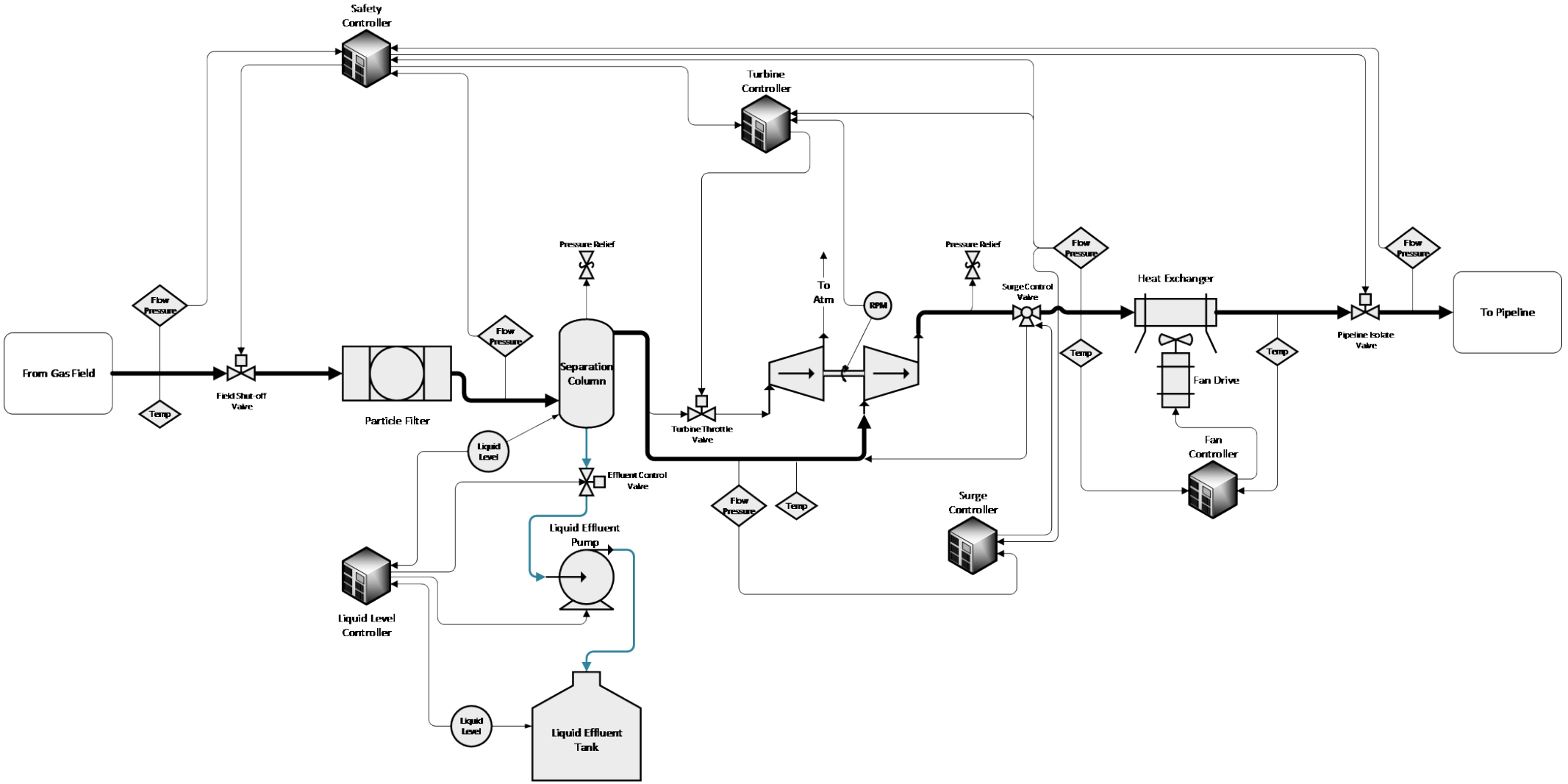
Physics Simulation Engine

- Matlab Simulink and Flownex SE are currently implemented as compatible physics simulators
- Physics data is read and written in real time to simulation environments based off of OT system feedback
- Leverage discretized time synchronization between physics and PLC systems



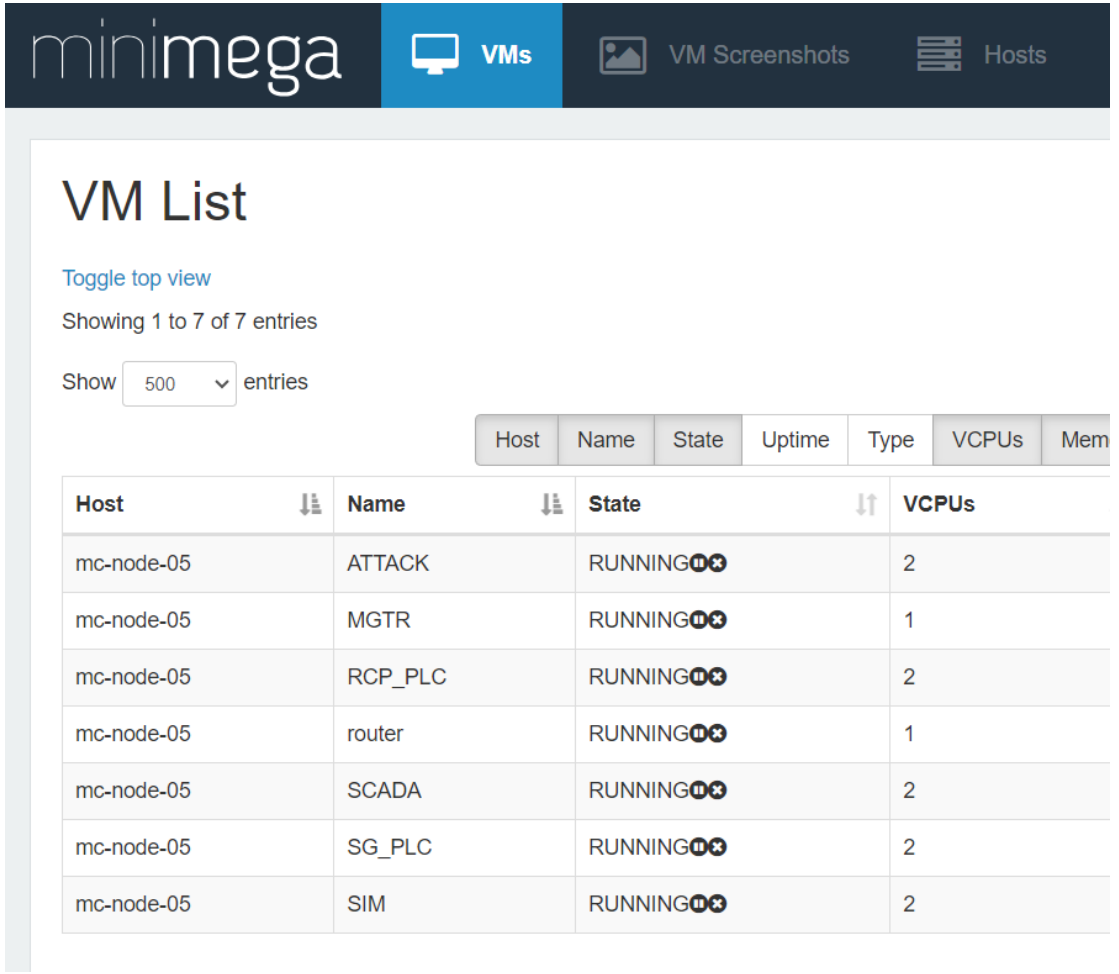
FLOWNEX®
SIMULATION ENVIRONMENT

Compressor Station Physics Modeling



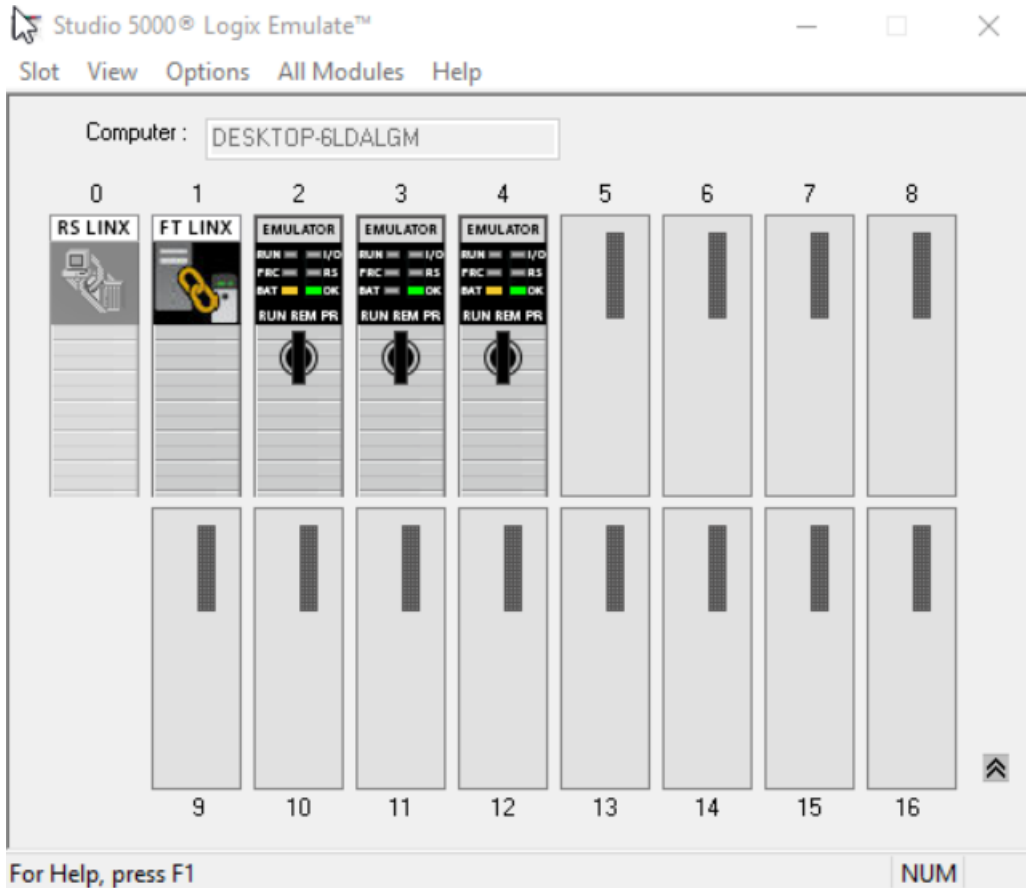
Network Simulation Engine

- Minimega serves as network simulator
- High transparency and scalability
- Ease of deployment across clusters or single machines
- Capacity for traffic generation simulation of various network conditions

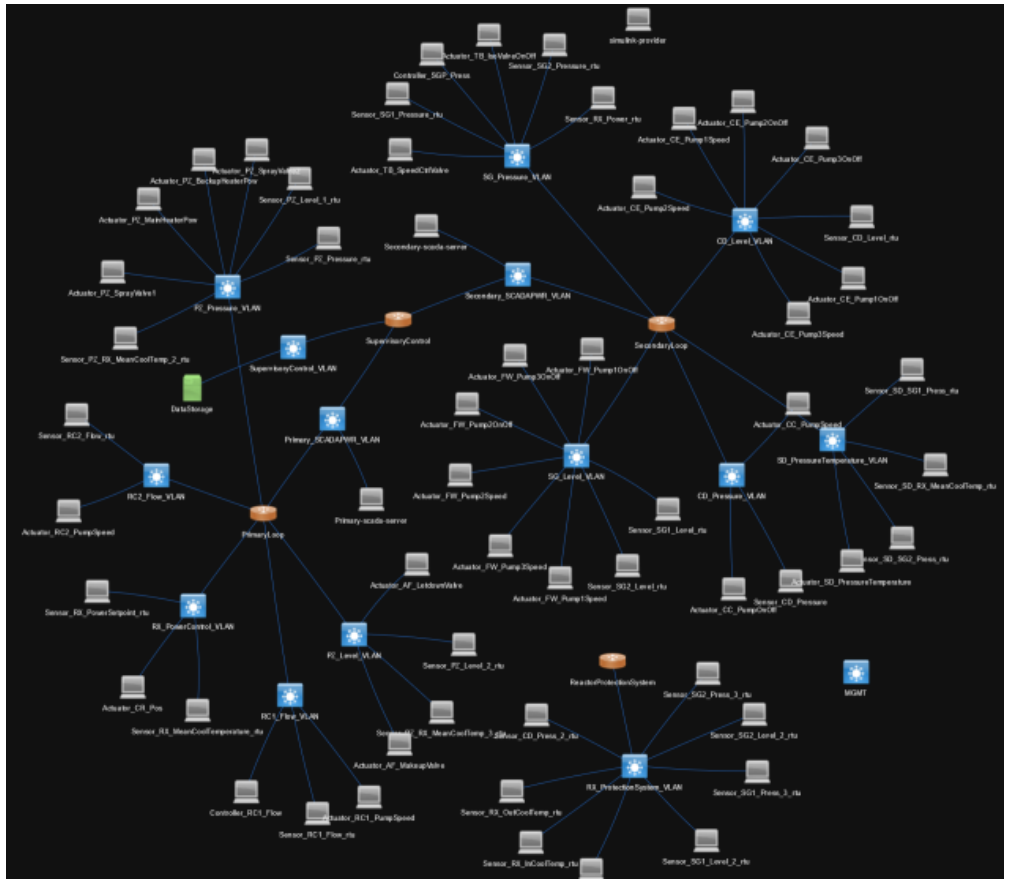


PLC Emulation Engine

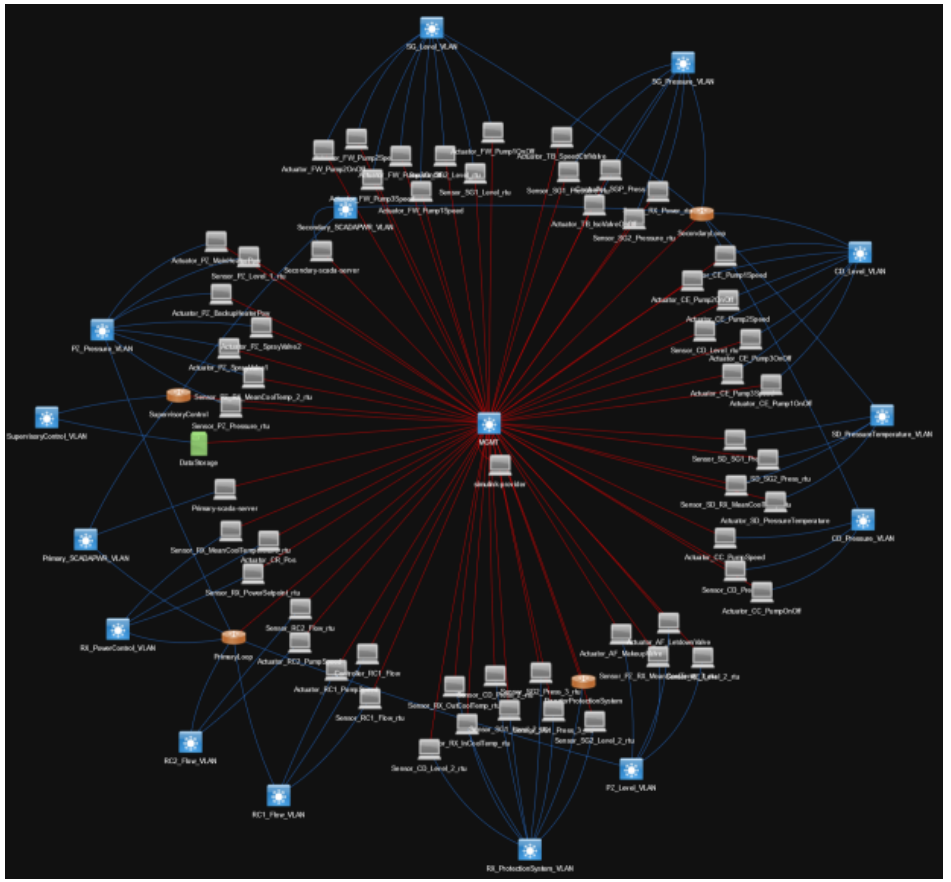
- PLC Emulation is performed on virtualized endpoint devices
- Existing tools such as Siemens PLCSim and Logix Emulate are designed to be run on Windows
- Independently addressable through the usage of a bridged network adapter for virtual PLCs



Simulation Scalability Visualization

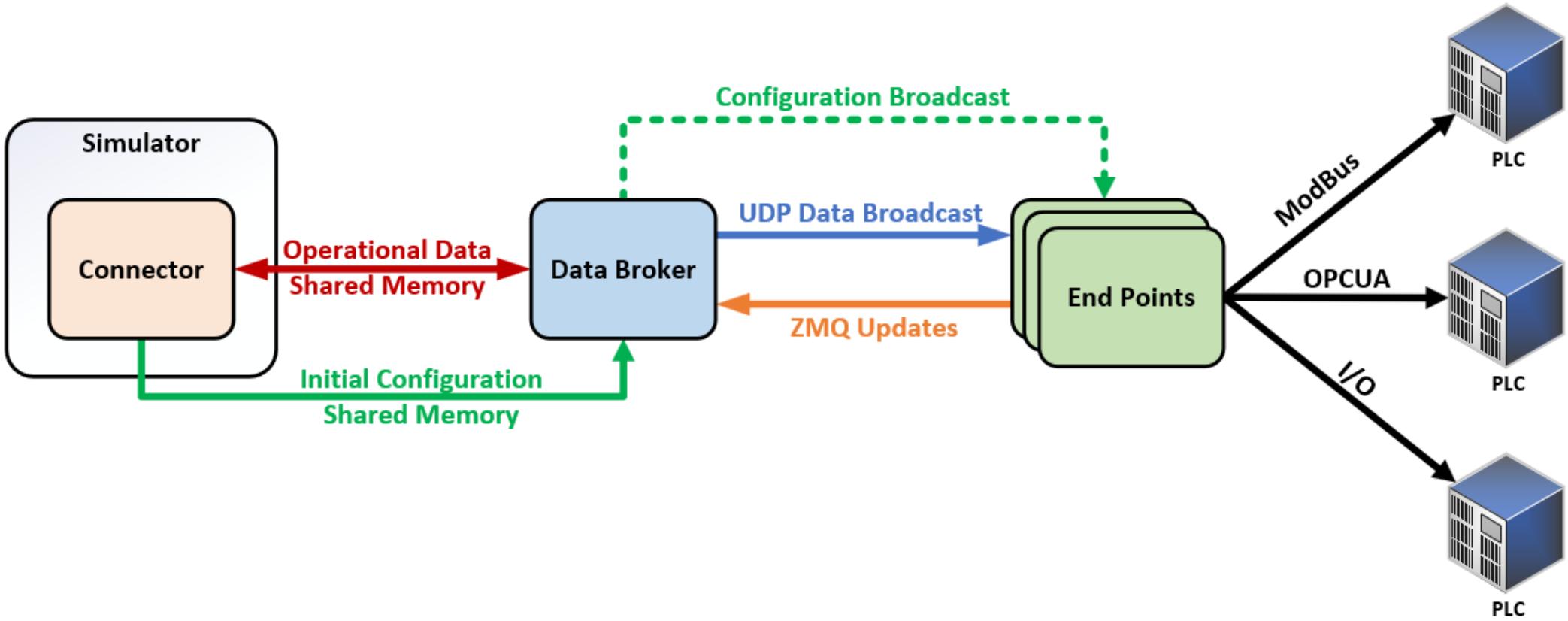


Controller Network



Management Network

The Data Broker exchanges data between the physics model and network emulation

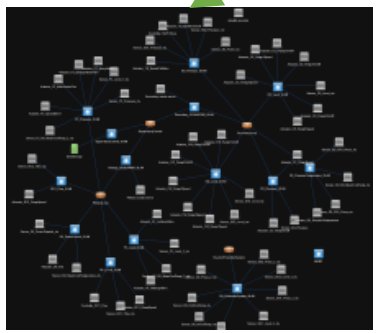


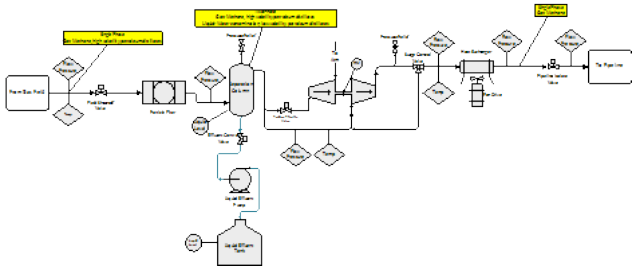
Analytical Tools

- Dakota - Sandia-developed data analysis tool
- Perform sensitivity analysis of key system outputs based on an array of potential cyber attacks
- Through Minimega, we conduct many runs across an array of input values for environment operation
- Can discover novel unsafe control actions (UCAs)

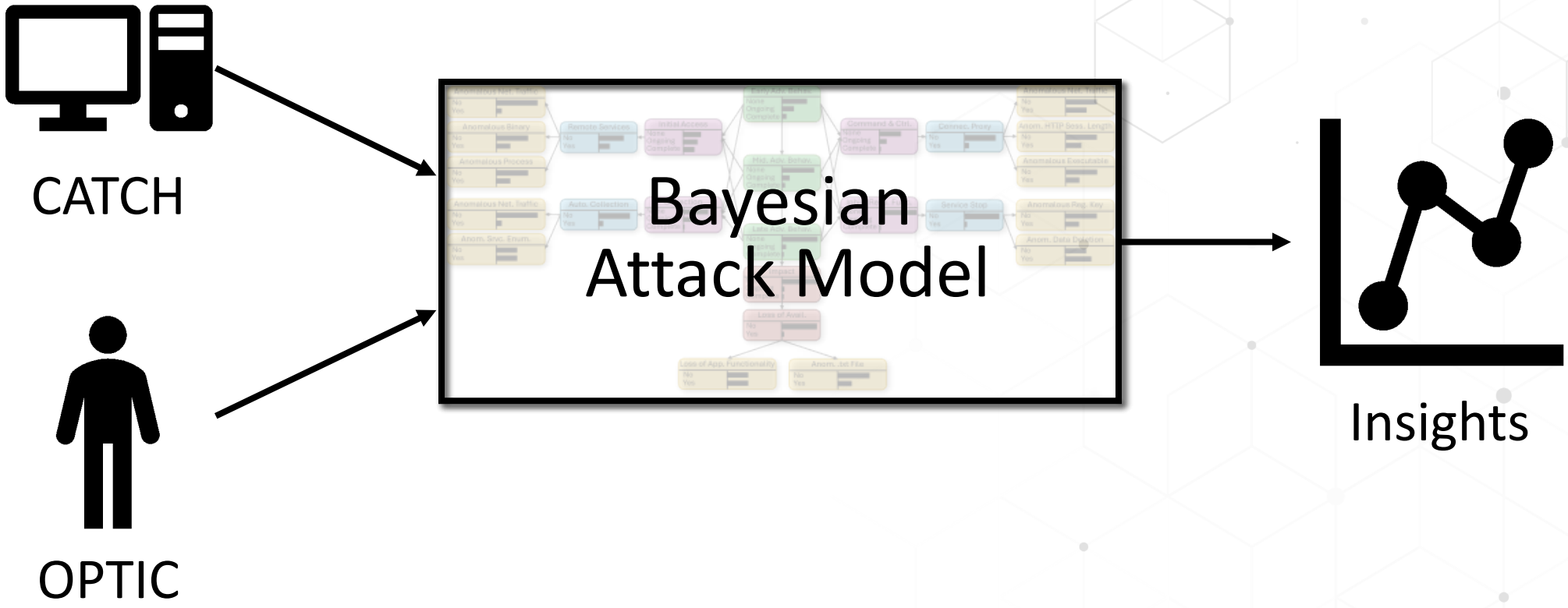
DAKOTA

Explore and predict with confidence.



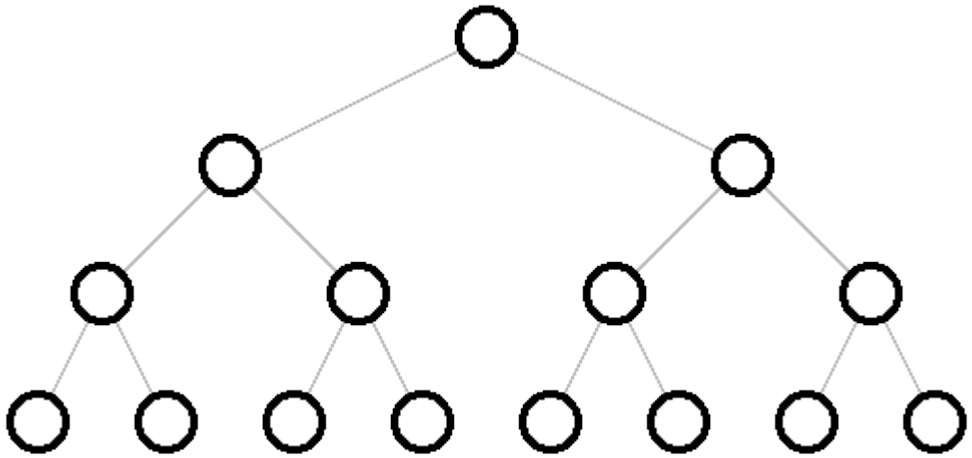


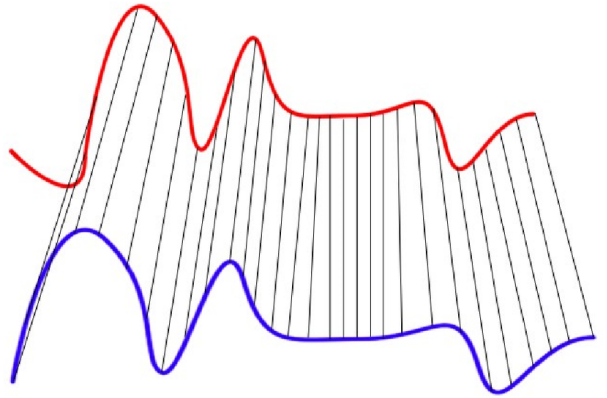
Testing OT Cybersecurity Tools



Additional AI Tools

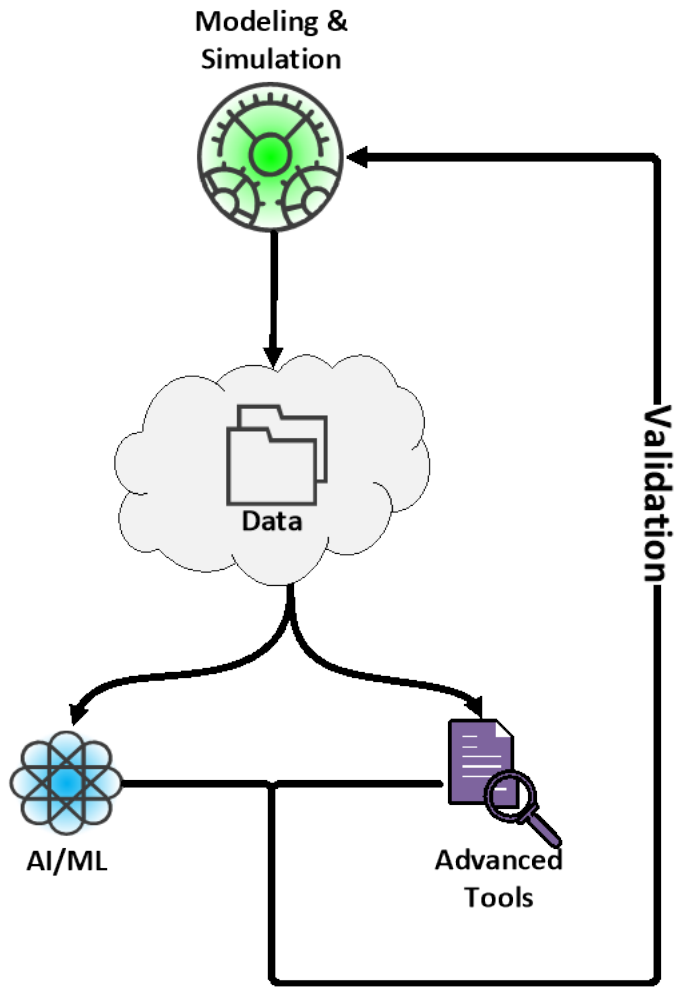
- Traditional sensitivity analysis tools such as Dakota may be aided by AI search space techniques
- Classification models may identify time series data for attacks and normal operations
- Semi-supervised techniques allow for model development on a smaller, labeled set of data





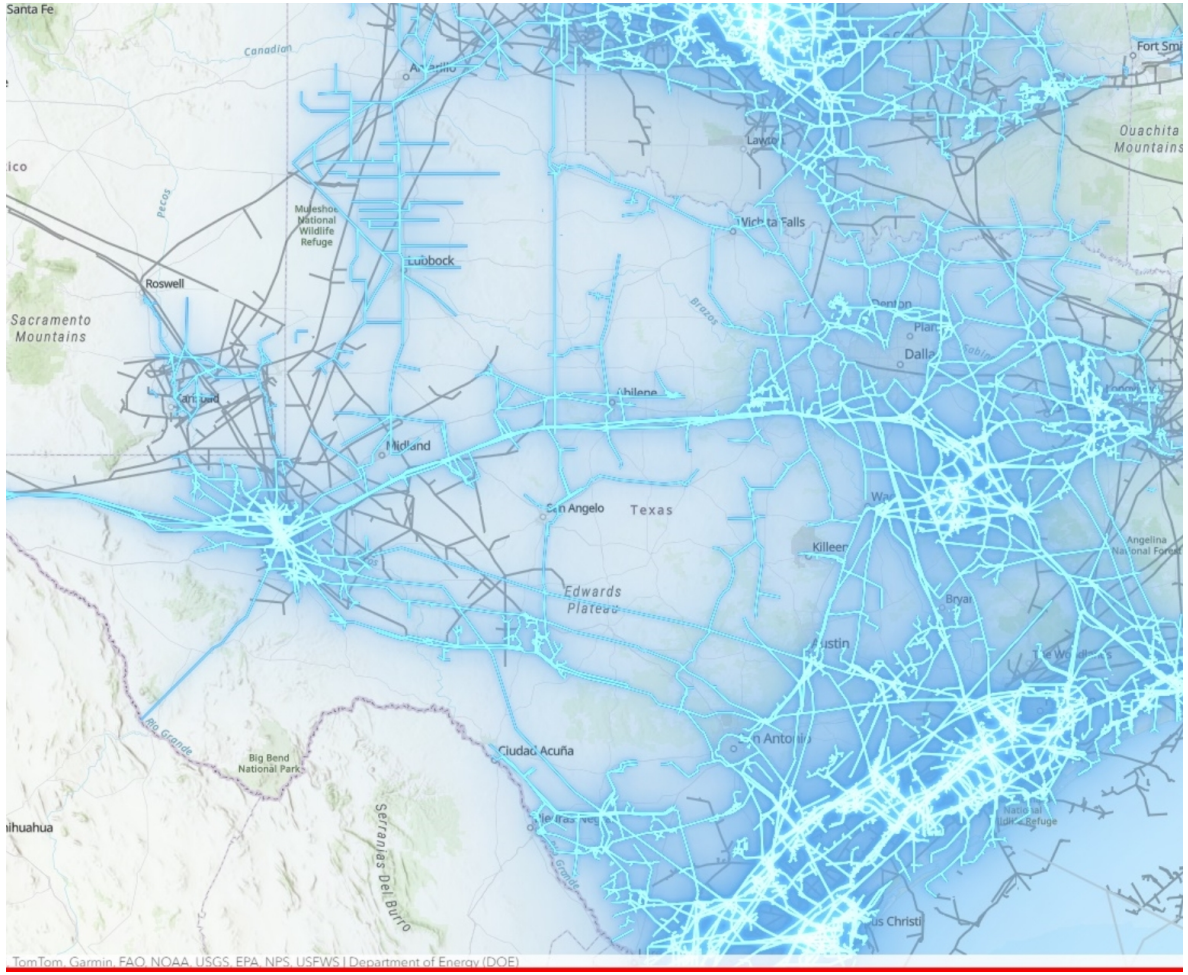
Workflow Outputs

- These tools allow for a cyclical workflow of attack discovery and patching
- Draws on simulation scalability and repeatability
- Allows for generation of large OT environment datasets
- These insights guide future work and experimentation



Future Work

- Complete V&V plan and conduct experiments
- Integrate modeling and simulation environment into cyber analysis system
- Increase scope of mod/sim to pipeline scale
- Identify AI/ML integration and experimentation opportunities



https://www.arcgis.com/apps/mapviewer/index.html?layers=3039af74880b4e8ea616b8fcdc2cc52d

For questions contact:

Lee T. Maccarone, lmaccar@sandia.gov

Coauthors: Adam J. Beauchaine, Titus A. Gray, Andrew S. Hahn, Scott T. Bowman

@DOE_CESER

linkedin.com/company/office-of-cybersecurity-energy-security-and-emergency-response

energy.gov/CESER

This presentation was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy. INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.

U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response