SAND2021-10072C

Cyber Threat Modeling

Approaches and Tradeoffs

Eric Vugrin, Meghan Sahakian, and Jamie Thorpe
Sandia National Laboratories

Threat Modeling and Medical Device Cybersecurity, a National Security Perspective

Center for Medical Device Cybersecurity, University of Minnesota

August 24, 2021

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.

Outline

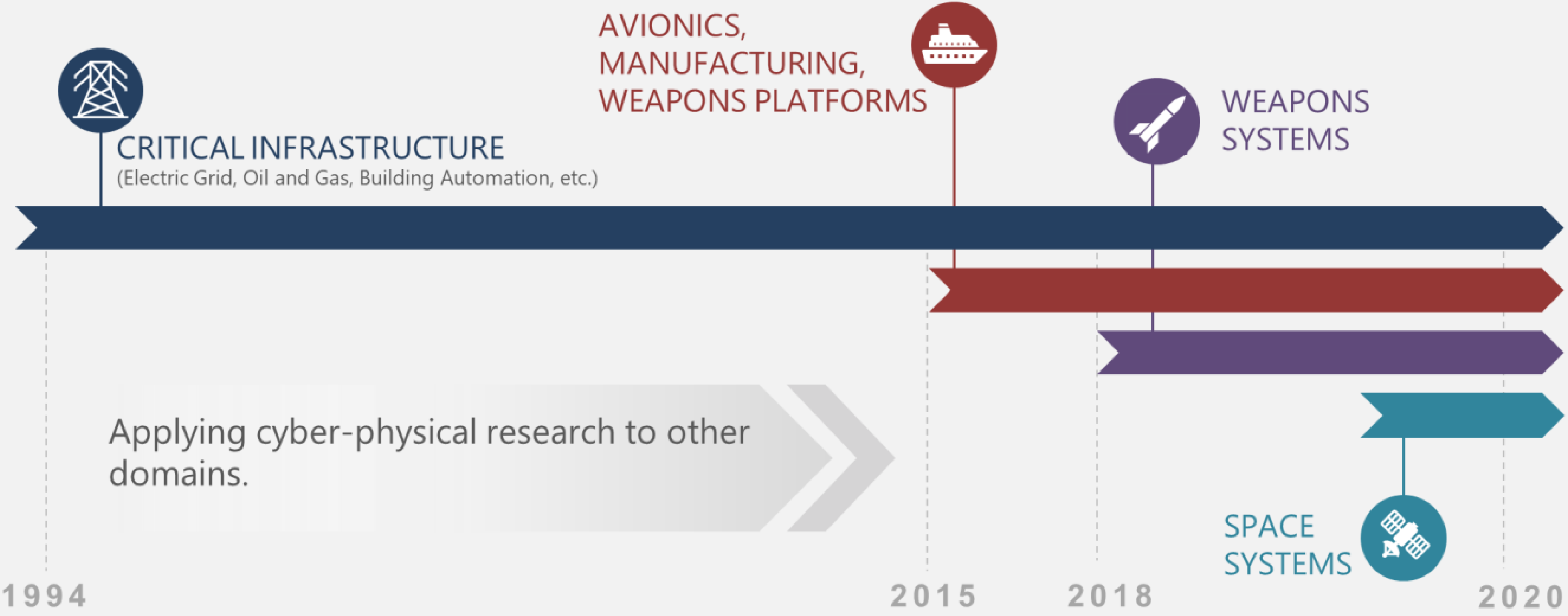
- Introduction
- Cyber Threat Modeling Process and Approaches
- Virtual Testbeds
- ADROC: ADvancing Resilience Of Control Systems
- Summary and Recommendations

Sandia National Laboratories

- Established in 1949
- Federally funded research and development center
- Managed by National Technology and Engineering Solutions of Sandia for US Department of Energy
- National security mission includes cybersecurity elements

Sandia's Major Program Portfolios

Timeline of Cyber-Physical R&D at Sandia



Modeling and simulation is a core capability of our cyber-physical research at Sandia.

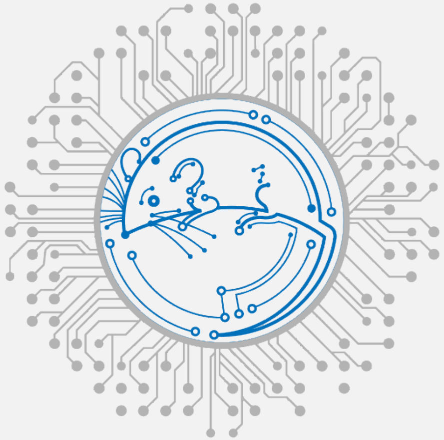
Examples of Cyber-Physical Modeling Activities

Exercises and Training

MOSAICS

Situational Awareness & Security

Intrusion Detection



Enhanced Rigor for Cyber Experimentation

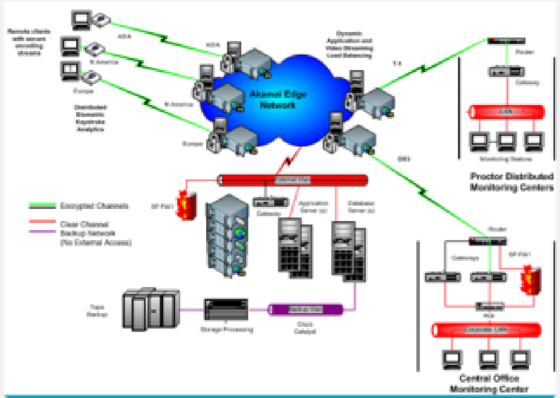
Despite the different applications, model development follows a common set of steps.

Step 1: ID questions to be addressed

These questions inform many of the modeling decisions modelers have to make

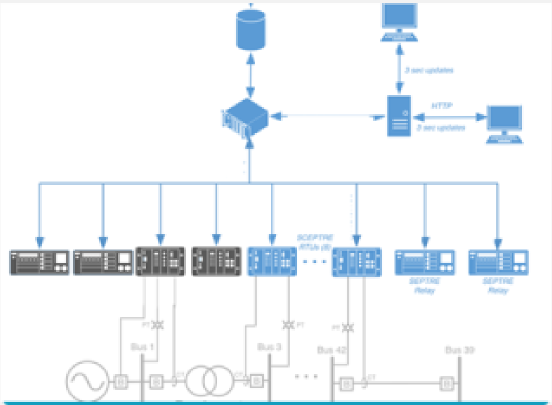
- Scope (elements represented)
- Higher/lower fidelity elements
- Threat-system interactions
- Model outputs

Step 2: Consider possible modeling approaches



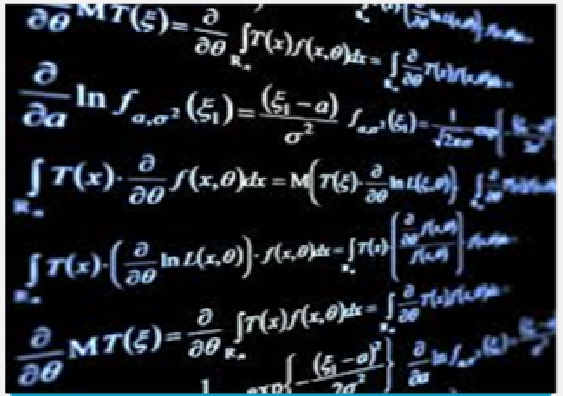
ACTUAL SYSTEM

REAL HARDWARE
REAL SOFTWARE



VIRTUALIZED TESTBED

ABSTRACT HARDWARE
REAL SOFTWARE



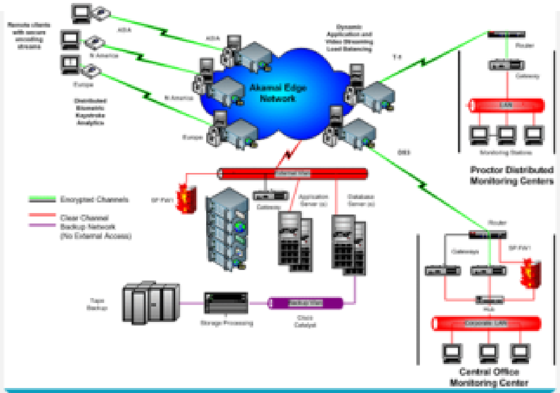
SIMULATION

ABSTRACT HARDWARE
ABSTRACT SOFTWARE

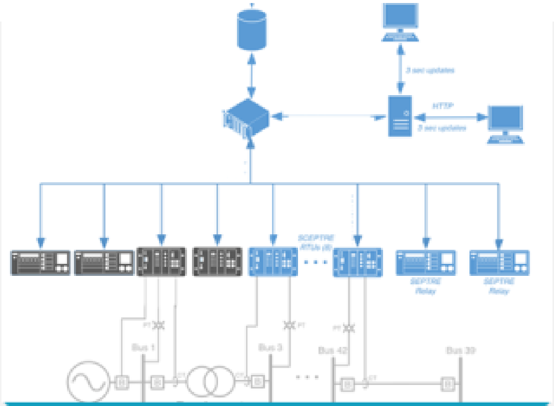
"BAD DAY" BRAINSTORMING

SUBJECT MATTER
EXPERT-DRIVEN

Step 3: Compare approaches vs. needs/constraints



ACTUAL SYSTEM



VIRTUALIZED TESTBED

SIMULATION

"BAD DAY" BRAINSTORMING

Increasing Realism
Decreasing Flexibility
Increasing Cost
Increasing Time

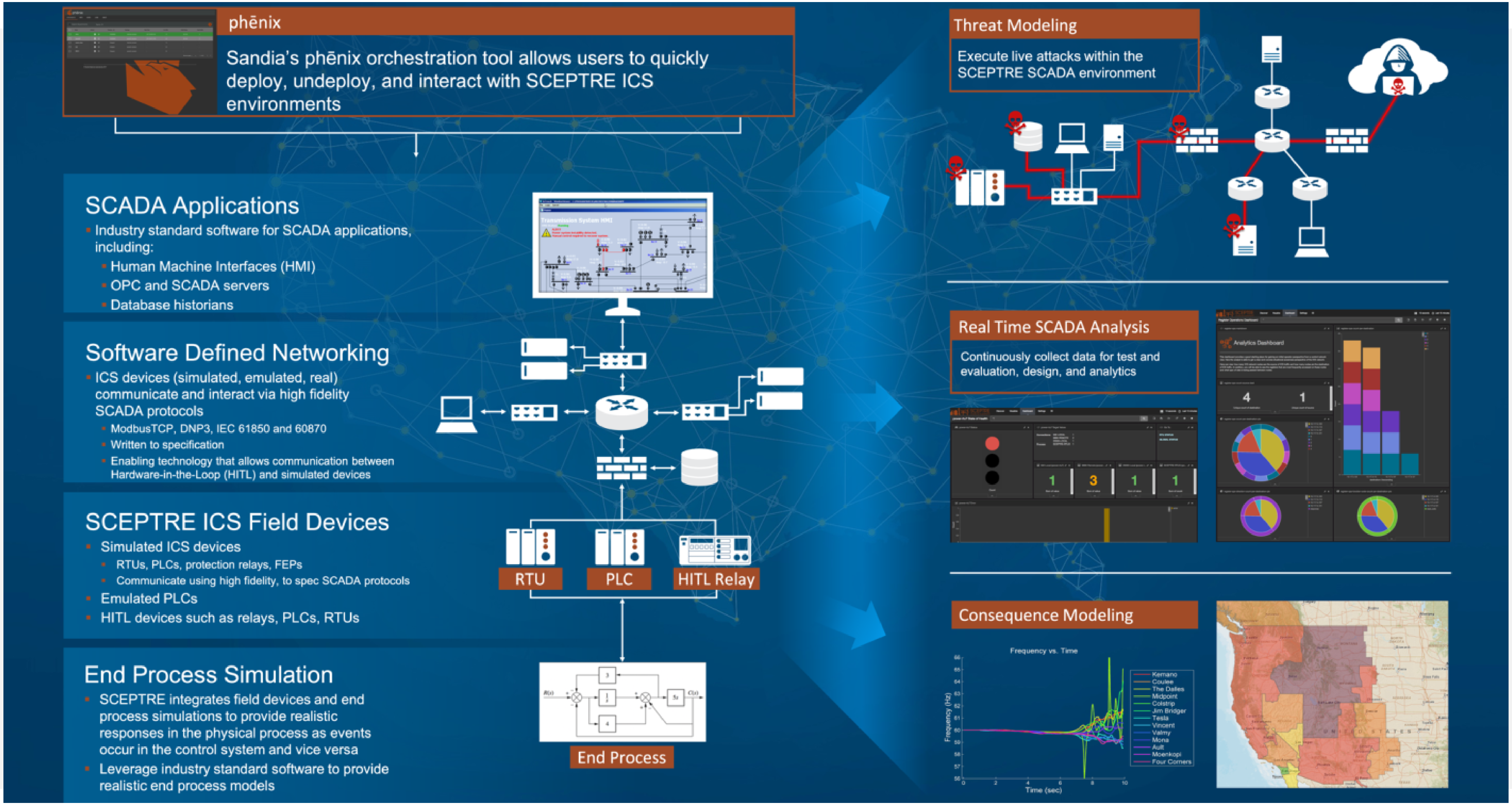
Increasing Abstraction
Increasing Flexibility
Decreasing Cost
Decreasing Time

Technical requirements vary across approaches,
but need for system and threat SMEs is common.

Virtual Testbeds, i.e., Emulation

- Often provides balance of realism and flexibility
- Can consist of
  - Virtual machines
  - Real software, operating systems, communication protocols
  - Can connect with simulation of physical (or biological) process
  - Can include hardware-in-the-loop (if needed)
  - Threat vector (real or emulated)
- Provides safe environment for threat investigation
  - Realistic threats (e.g., actual malware) or actual attacks
  - Won’t cause actual damage
  - Can observe effects of attack
  - Spin up/tear down environment as needed

SCEPTRE: Emulation of Cyber-Physical Systems



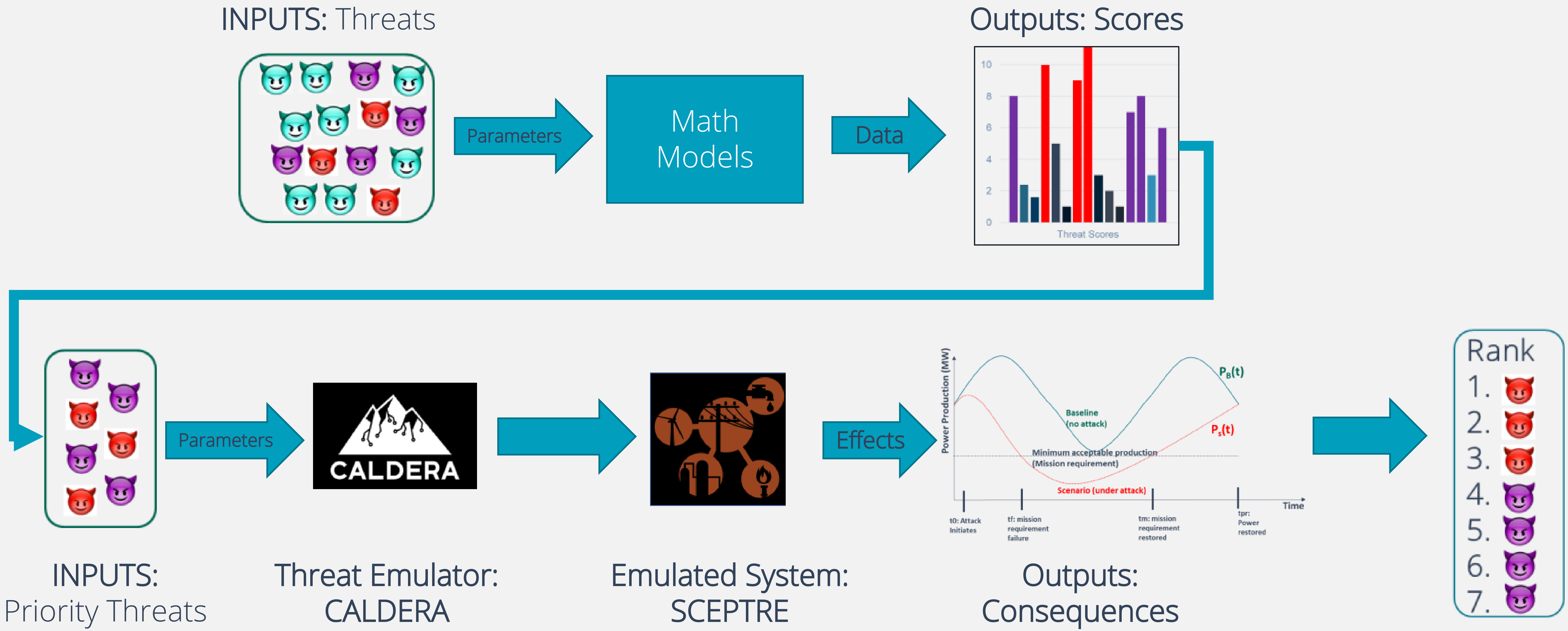
Use Cases

- Training and exercise support
- Mission rehearsal
- Test and evaluation
- Analysis: vulnerabilities, criticality, dependencies, malware sandbox
- Challenges
  - Operates in real-time which can be time-limiting
  - Significant learning curve
  - Heterogeneity of devices may present challenges
  - Validation of results?

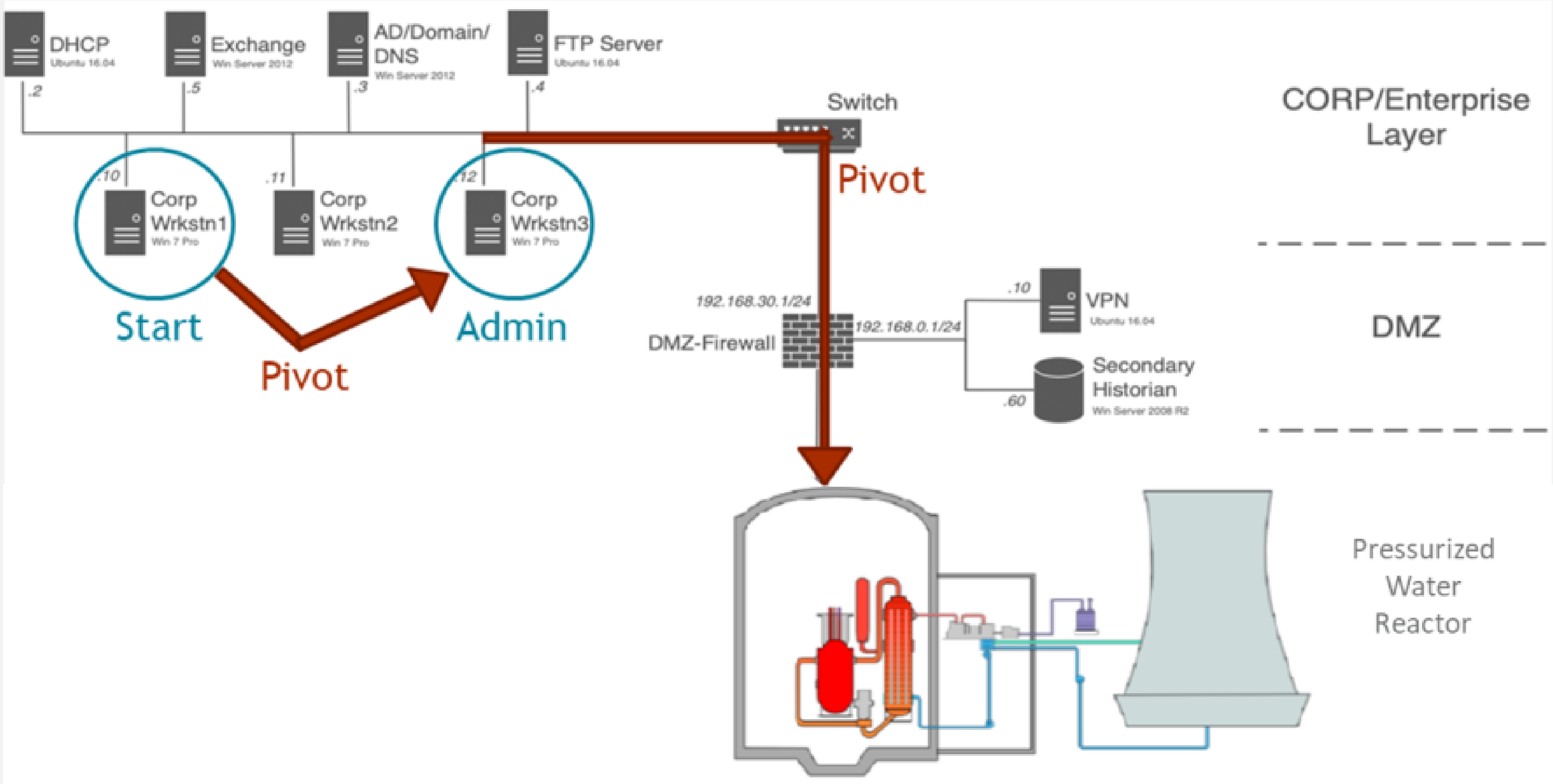
ADROC: ADvancing Resilience Of Control Systems

- New research effort
- Goal: develop cyber experimentation platform for quantitative analysis and characterization of threats to industrial control systems (ICS)
- Approach: mathematical and emulation modeling

ADROC Project

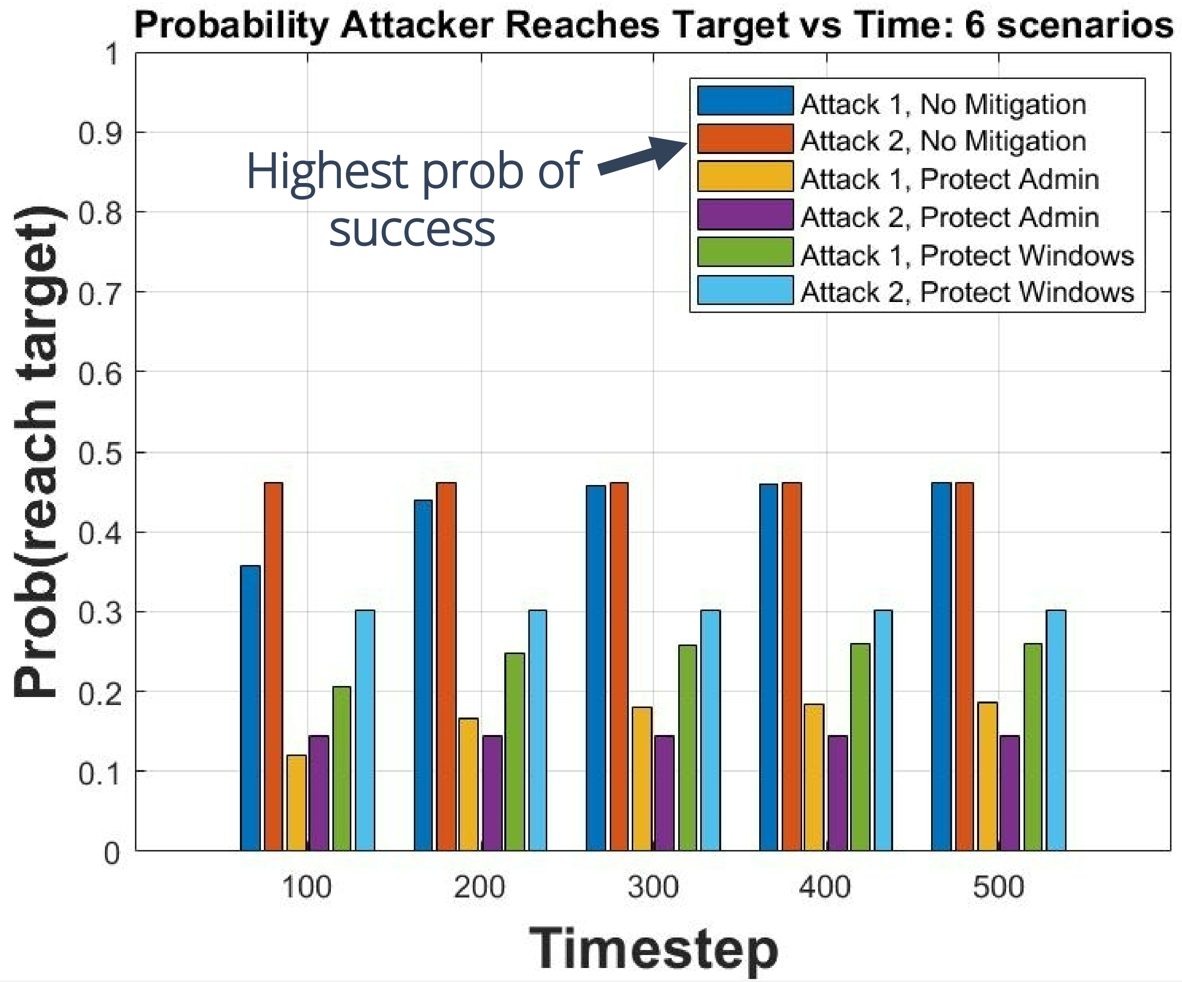


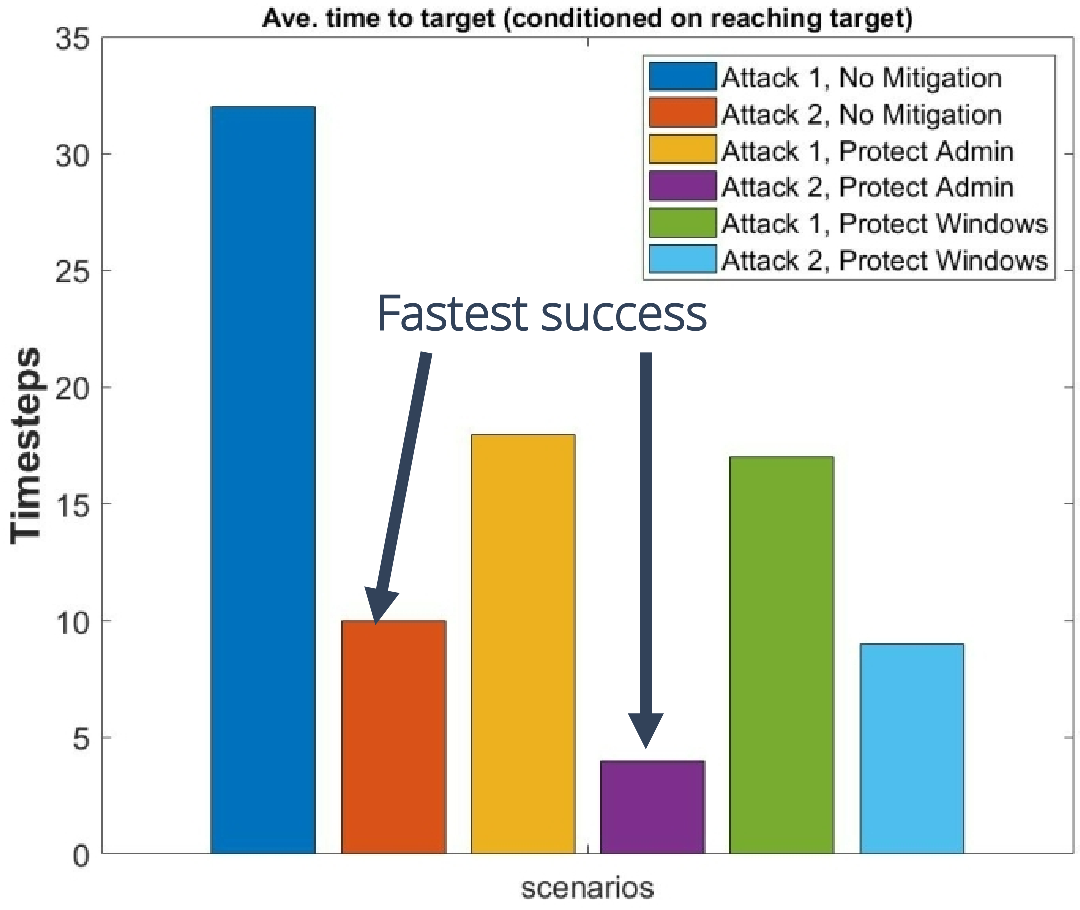
Scenario: Attack on Nuclear Power Plant



Attacker goal: cause unsafe conditions

Math Modeling: Example Results



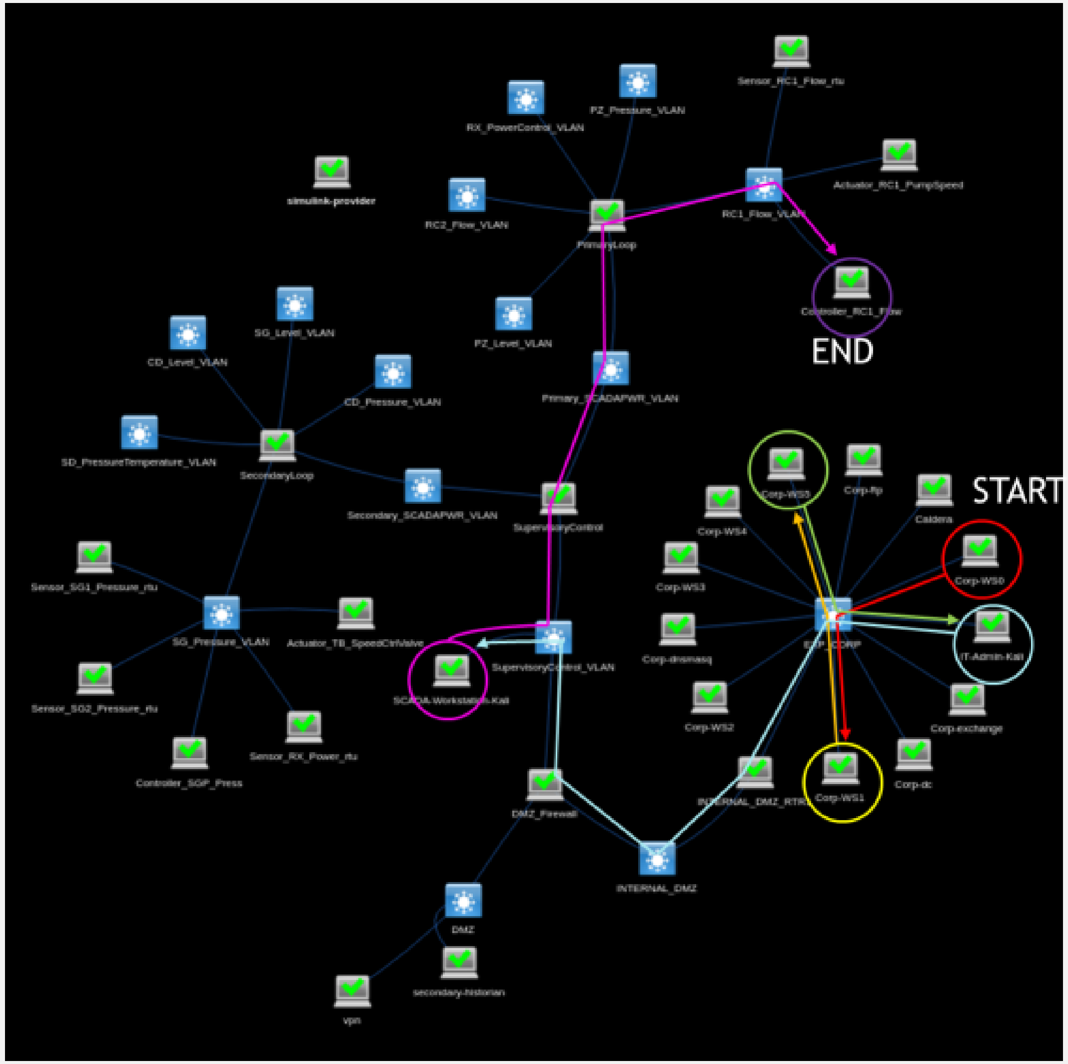


Limitation: fast but can't determine impact of attack

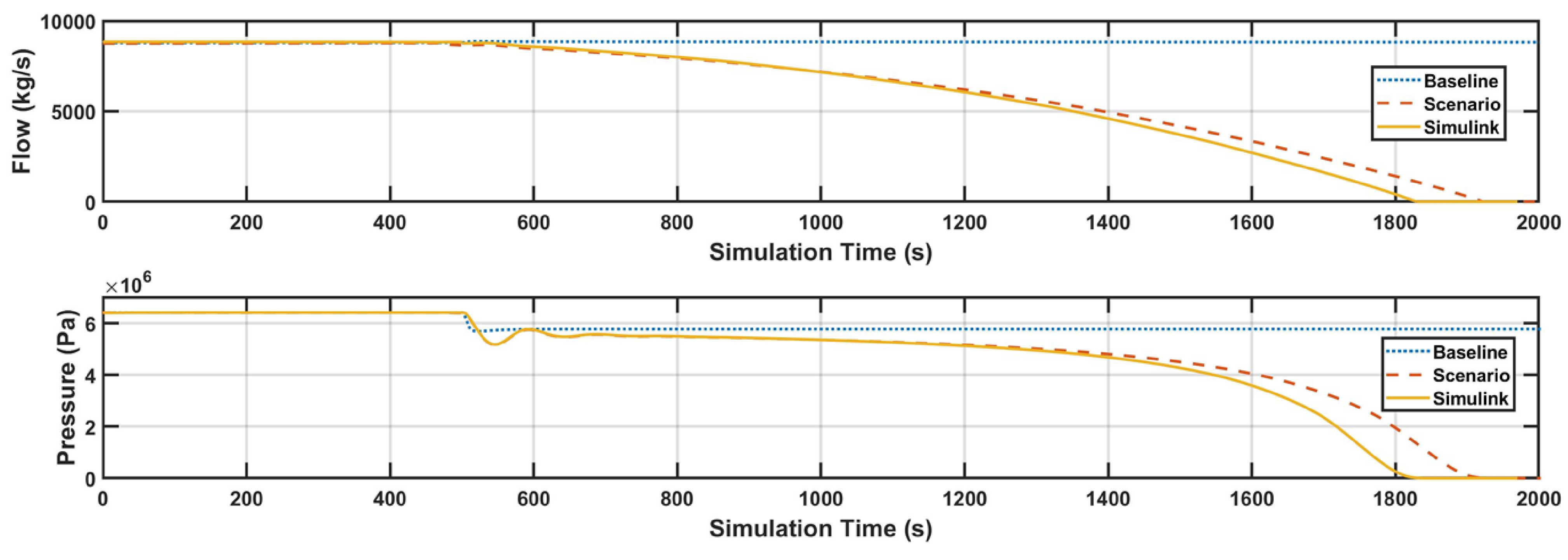
Emulation Modeling: Example Results

Emulation allows us to

- Track movement of malware
- Observe targeted device
- Quantify effect of attack



Emulation Modeling: Example Results



Attack destabilizes pressure and flow

*Figures from Hahn, et al., "Automated Cyber Security Testing Platform for Industrial Control Systems," 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies, 2021.

Summary

- Several approaches exist for modeling cyber threats
- Virtual testbeds (emulation) are an emerging technology that provides a “safe” environment for cyber threat investigation
- The ADROC project is using a hybrid modeling approach to enable efficient AND “validate-able” prioritization of threats

Recommendations

Before building a model

- Formally state the question you are trying to answer
- Develop a conceptual model of the system and threat
- Evaluate your needs and constraints (time, budget, capabilities)

Remember

- There is no single, perfect method
- Your answers will only be as good as your data permits
- Start slowly and eventually build in complexity

Thank you

Acknowledgments

ADROC team: Jamie Thorpe, Amanda Gonzales, Chris Mairs, Tim Ortiz, Meghan Sahakian, Eric Vugrin, Derek Hart

Nuclear Power Plant Modeling: Andrew Hahn, Ray Fasano, Tim Ortiz, Chris Lamb

ADROC is funded through Sandia's Laboratory Directed Research and Development programs.