SAND2019-4652PE

LDRD

Laboratory Directed Research and Development

SECURE: An Evidence-based Approach to Cybersecurity

Ali Pinar, PI

Zach Benz, PM

Contact: apinar@sandia.gov; zobenz@sandia.gov

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

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.

SECURE: **S**cience and **E**ngineering of **C**ybersecurity by **U**ncertainty quantification and **R**igorous **E**xperimentation

- Cyber experimentation is essential for securing cyber systems
  - collective behavior is hard to predict
  - experimenting on a real system is not an option
    - too risky, if possible
    - we design future systems

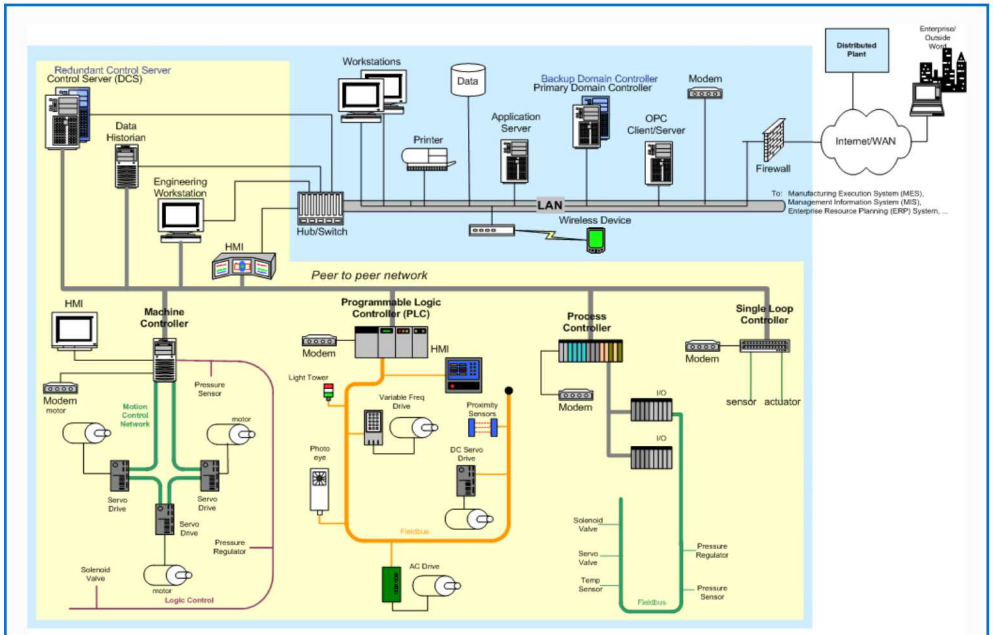
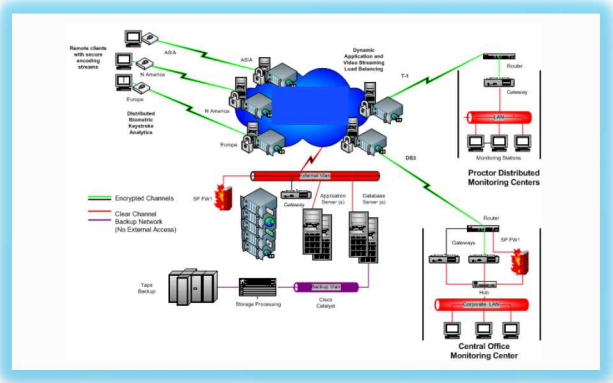


Figure 1: Generic Industrial Control System Network Architecture - DCS

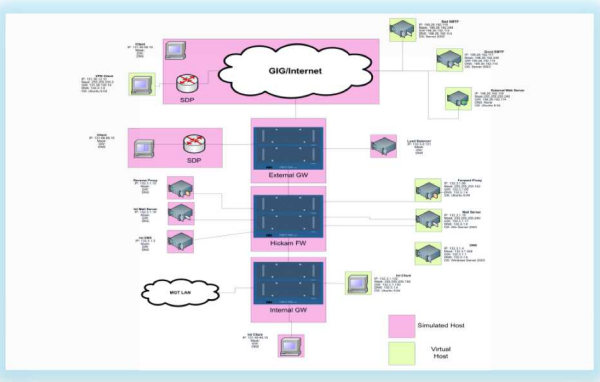
- Computational experimentation is a powerful tool
  - But lack of rigor limits adoption for high-consequence decisions

- Can we rigorously quantify security?
  - *"What is the probability that a message from The President will reach military units within x seconds?"*

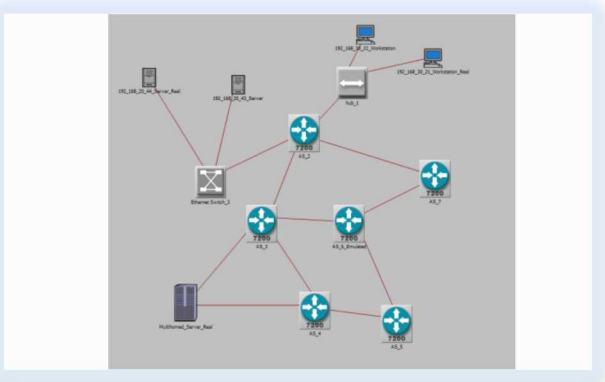
Cyber experimentation approaches



ACTUAL SYSTEM



VIRTUALIZED TESTBED



SIMULATION TESTBED

Interoperability in a single experiment

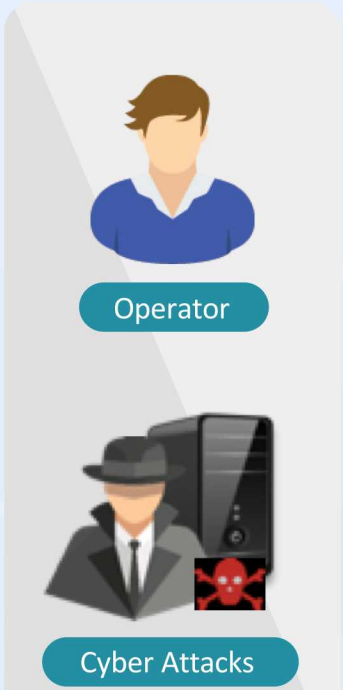
LIVE ← Increase Realism

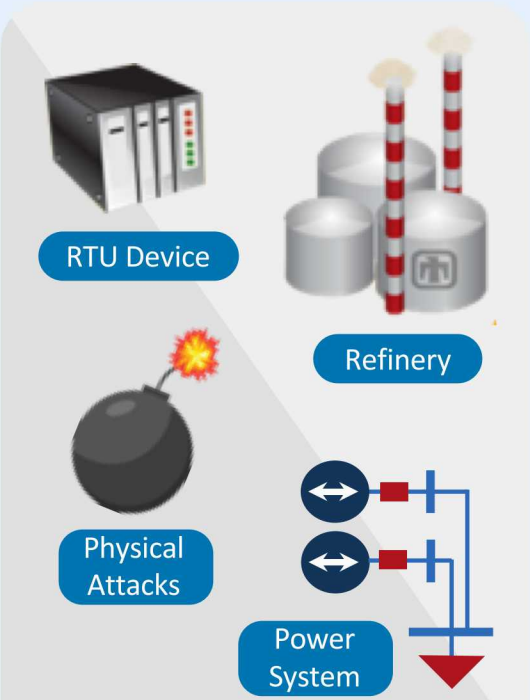
Decrease Cost, Decrease Time → SIMULATED

REAL HARDWARE REAL SOFTWARE	ABSTRACT HARDWARE REAL SOFTWARE	ABSTRACT HARDWARE ABSTRACT SOFTWARE

Emulytics:
Sandia's approach

What is Experimental Cyber?





HUMAN

HARDWARE IN THE LOOP

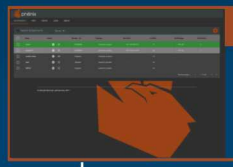
EMULATED

SIMULATED

SCEPTRE
scada-as-a-platform™

Sandia National Laboratories

SCEPTRE provides a comprehensive ICS/SCADA modeling and simulation capability that captures the cyber/physical impacts of targeted cyber events on critical infrastructure and control systems

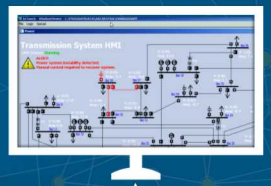


phēnix

Sandia's phēnix orchestration tool allows users to quickly deploy, undeploy, and interact with SCEPTRE ICS environments

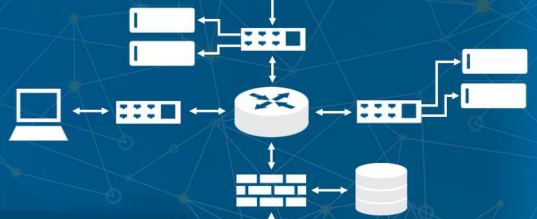
SCADA Applications

- Industry standard software for SCADA applications, including:
  - Human Machine Interfaces (HMI)
  - OPC and SCADA servers
  - Database historians



Software Defined Networking

- ICS devices (simulated, emulated, real) communicate and interact via high fidelity SCADA protocols
  - ModbusTCP, DNP3, IEC 61850 and 60870
  - Written to specification
  - Enabling technology that allows communication between Hardware-in-the-Loop (HITL) and simulated devices

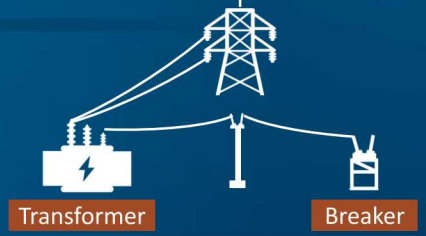


SCEPTRE ICS Field Devices

- Simulated ICS devices
  - RTUs, PLCs, protection relays, FEPs
  - Communicate using high fidelity, to spec SCADA protocols
- Emulated PLCs
- HITL devices such as relays, PLCs, RTUs

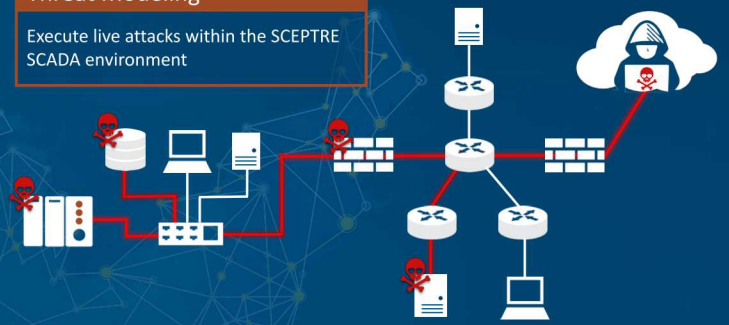
Power Simulation

- SCEPTRE integrates field devices and power simulations to provide realistic responses in the physical process as events occur in the control system and vice versa
- Leverage industry standard software to provide realistic end process models



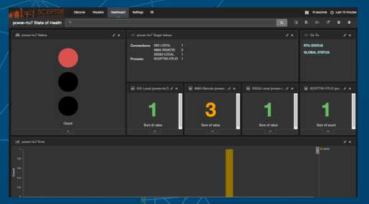
Threat Modeling

Execute live attacks within the SCEPTRE SCADA environment

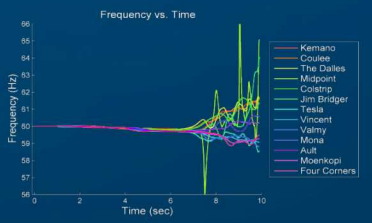


Real Time SCADA Analysis

Continuously collect data for test and evaluation, design, and analytics



Consequence Modeling



RTU – Remote Terminal Unit
PLC – Programmable Logic Controller

OPC – OLE for Process Control
SCADA – Supervisory Control And Data Acquisition

ICS – Industrial Control System

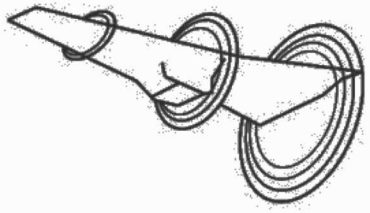
timission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly nal, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

NNSA National Nuclear Security Administration | U.S. DEPARTMENT OF ENERGY

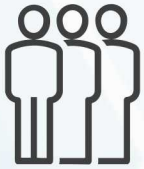
SECURE's Goal: Rigorous Cyber Experimentation

PHYSICS

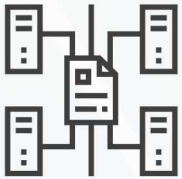
$F=ma$
$e=mc^2$
...
...

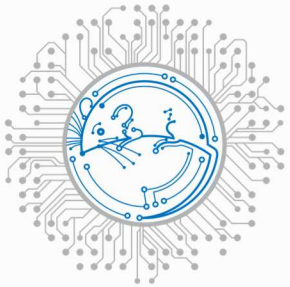


BIOLOGY



CYBER





EMULYTICS

SECURE: CYBER DECISION & DESIGN SUPPORT WITH RIGOR

The need is indisputable, the solution is elusive

"Most [cybersecurity] techniques are domain- and context-specific, often not validated as mathematically and empirically sound, and rarely take into account efficacy and efficiency. Thus, the state of the practice consists of heuristic techniques, informal principles and models of presumed adversary behavior, and process-oriented metrics."
– The 2016 Federal R&D Strategic Plan

State of the Art:

- Focus on the importance of the problem, as opposed to the solution
- Relying on heuristics and SME intuition
- Considered to be an engineering problem, not science
- Our approach: Follow the footsteps of computational science to bring rigor into cyber experimentation.

Bringing Rigor into Cyber Experimentation: The Plan in a nutshell

The Goal: Bring rigor into cyber experimentation

The Idea: Follow the principles of Computational Science and Engineering (CSE)

The Challenge: Cyber systems are different than those in traditional CSE applications.

The Plan:

- Build on our current strengths in core capabilities
  - Emulytics, Uncertainty Quantification (UQ), Optimization
- Advance the state of the art in core capabilities
  - e.g., multi-fidelity Emulytics, UQ in discrete domains; scalable solvers for adversarial optimization
- Integrate core capabilities over a power grid exemplar

Challenge is bringing together disparate strengths

- Predict:
  - **Emulytics:**
    - Investments for >10 years
    - Developed tools (Firewheel, minimega, SCEPTRE)
- Assess confidence:
  - **Uncertainty Quantification:**
    - Integral part of the ASC program and its success
    - Developed tools such as Dakota, UQTk
- Make robust decisions:
  - **Adversarial Stochastic Optimization:**
    - Optimization with discrete variables has long been a distinguishing Sandia strength
    - Widely used for infrastructure security

EMULYTICS

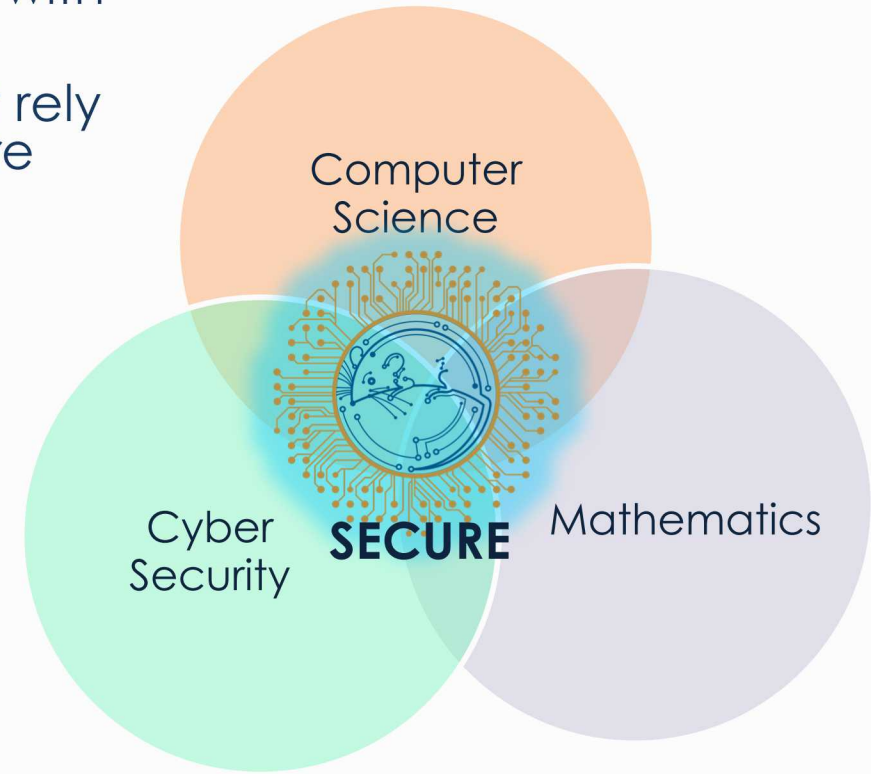
DAKOTA

PYOMO

2016 R&D 100 WINNER

How are cyber system models different?

- Challenge: A domain that violates underlying assumptions for the current tools
- Lack of first-principles or closed form governing equations.
  - Model/recreate individual components with virtualized hardware, real software
  - Different than agent-based models that rely on abstraction of hardware and software
- Discreteness/discontinuities
  - High number of binary variables
  - Discontinuities in the response surfaces
- Sources and dimensionality of uncertainty
  - E.g., network inference: presence/absence of a router
  - Irreducible uncertainties: adversary behavior
  - Each network entity is another dimension



Dealing with high dimensionality

- **Multifidelity approaches**
  - Take a large number of low fidelity runs and a small number of high fidelity runs to achieve statistics on high fidelity responses
    - Low fidelity runs are assumed to have bias
  - Relies on variance reduction: must have correlation between the low and high fidelity model

Fidelity definition

- `minimega` – HF: 100 Requests (average over 10 repetitions)
- `ns3` – LF: 10 Requests (`Delay` $50ms$)
- `ns3` – LF*: 1 Requests (`Delay` $5ms$)

	$\mathcal{C}$
HF	1
LF	0.016
LF*	0.002

TABLE: Normalized Cost

We assume **serial execution for the low-fidelity model**, however we might easily increase the efficiency of LF (`ns3`) by running multiple concurrent evaluations

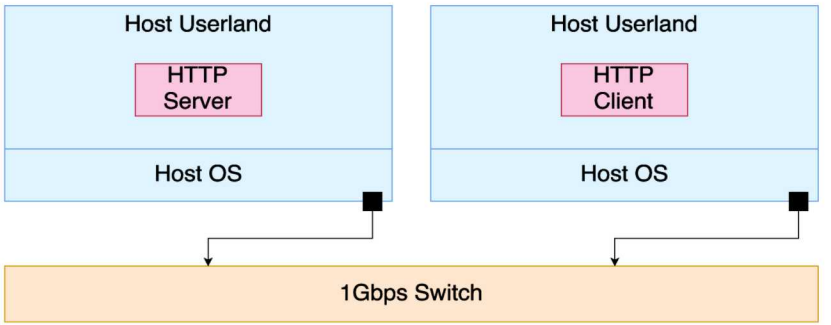


FIGURE: Network Configuration

Multi-fidelity modeling results – variance reduction

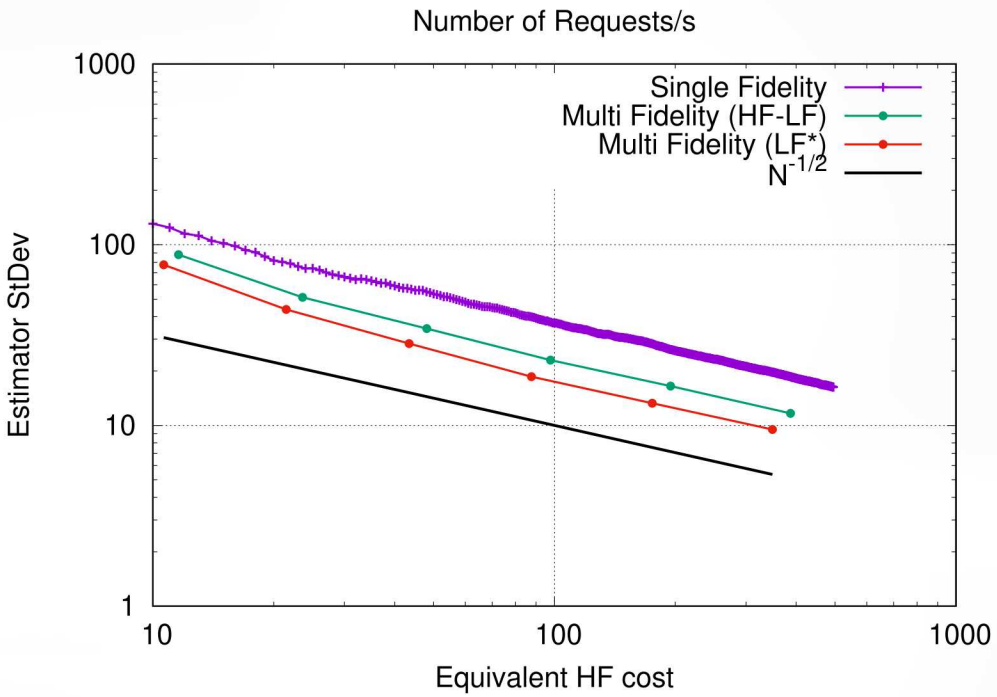


FIGURE: Exp. Value StDev

Example (for LF*)

- Number of **HF runs**: $N = 500$
- Number of **LF* runs**: $r_1 \times N = 5415$
- Equivalent **LF cost**: $r_1 \times N \times \dfrac{\mathcal{C}_{LF}}{\mathcal{C}_{HF}} = 11$
- **Total** estimator **cost** (HF + LF*): $\mathcal{C}_{tot} = 500 + 11 = 511$
- **Variance reduction**: $\left(1 - \dfrac{r_1 - 1}{r_1}\rho_1^2\right) = 0.23$

- The **variance reduction** we obtain w.r.t. MC is

$$\mathbb{V}ar\left(\tilde{Q}\left(\underline{\alpha}^{ACV}\right)\right) = \mathbb{V}ar\left(\hat{Q}\right)\left(1 - \frac{\mathbf{r_1 - 1}}{\mathbf{r_1}}\rho_1^2\right)$$

- The **number of low-fidelity simulations** is $N_{LF} = N \times r_1$ where

$$r_1 = \sqrt{\frac{\mathcal{C}_{HF}}{\mathcal{C}_{LF}}\frac{\rho_1^2}{1 - \rho_1^2}}$$

- For each HF simulation we need to spend an **extra cost** in LF simulations

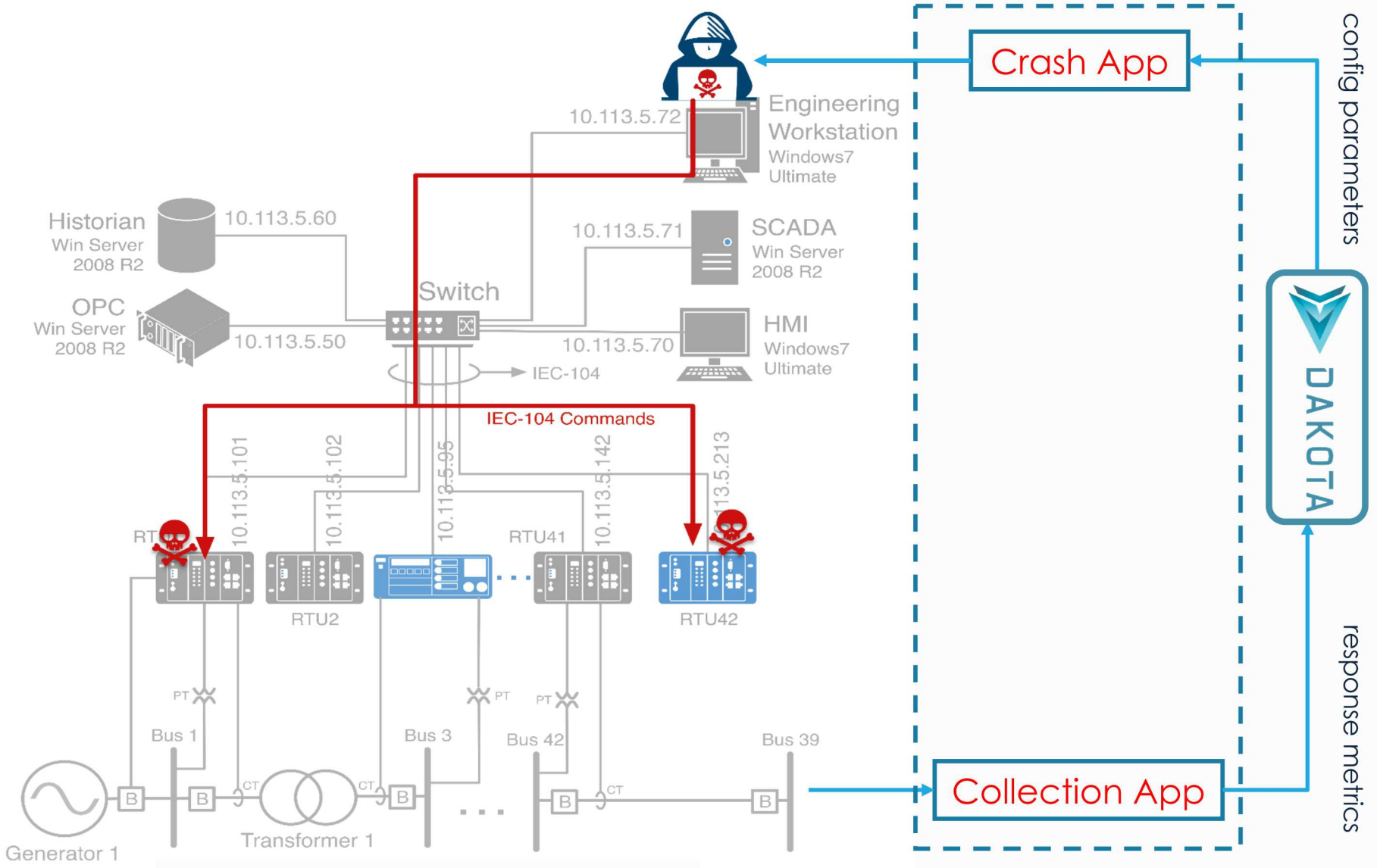
$$\text{Eq.Cost}: \quad \mathcal{C}_{tot} = N\left(1 + \mathbf{r_1}\frac{\mathcal{C}_{\mathbf{LF}}}{\mathcal{C}_{\mathbf{HF}}}\right)$$

- For this case

	ρ_1	r_1	$r_1\mathcal{C}_{LF}/\mathcal{C}_{HF}$
LF	0.86	4.69	0.075
LF*	0.90	10.83	0.022

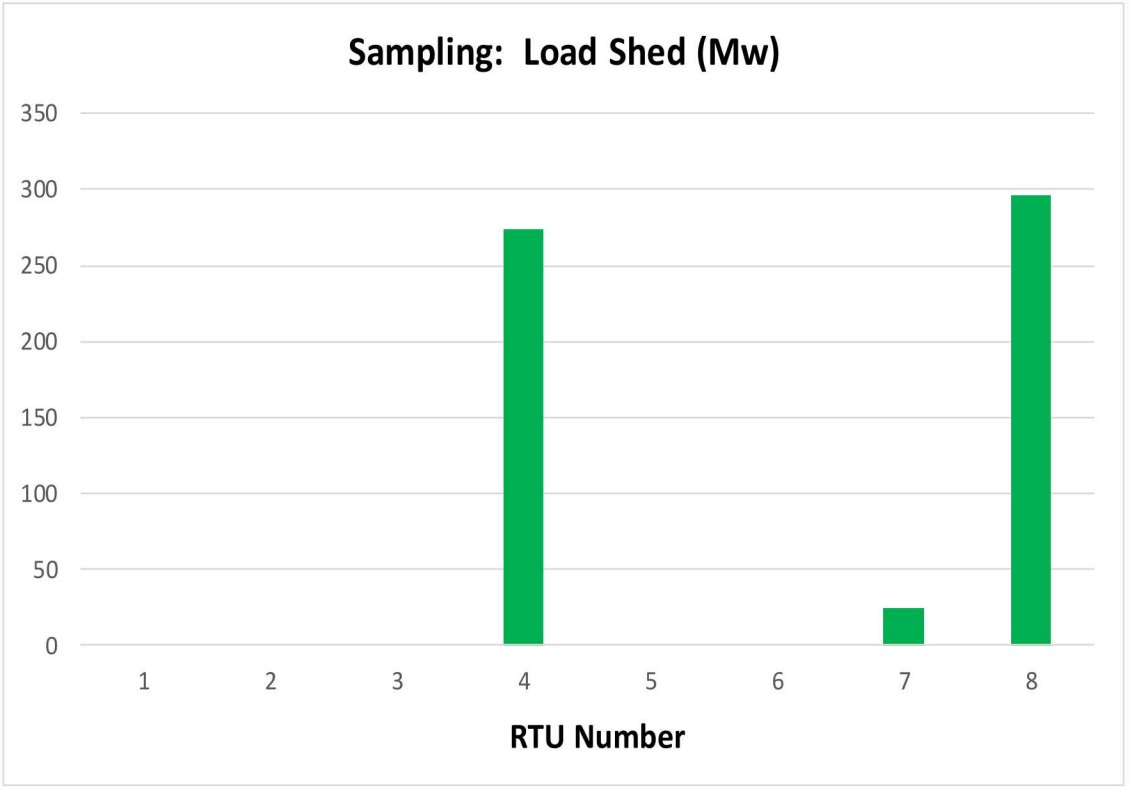
More than 70% variance reduction is obtained by adding **only an equivalent cost of 11 HF runs.**

Studies on a SCADA network: What may happen?



Results: Impacts on Varying Target RTU

- There is variation in load shed when we target one RTU at a time
- Only three of the RTUs (#4, 7, and 8) generate effects on the response metric
- Results indicate that RTU-8 is a high-priority RTU for protection (followed closely by RTU-4)
- Given a limited budget, defender should not prioritize RTUs 1, 2, 3, 5, and 6



*Derived from synthetic data with no relation to actual grid: https://electricgrids.engr.tamu.edu/electric-grid-test-cases/activsg2000/

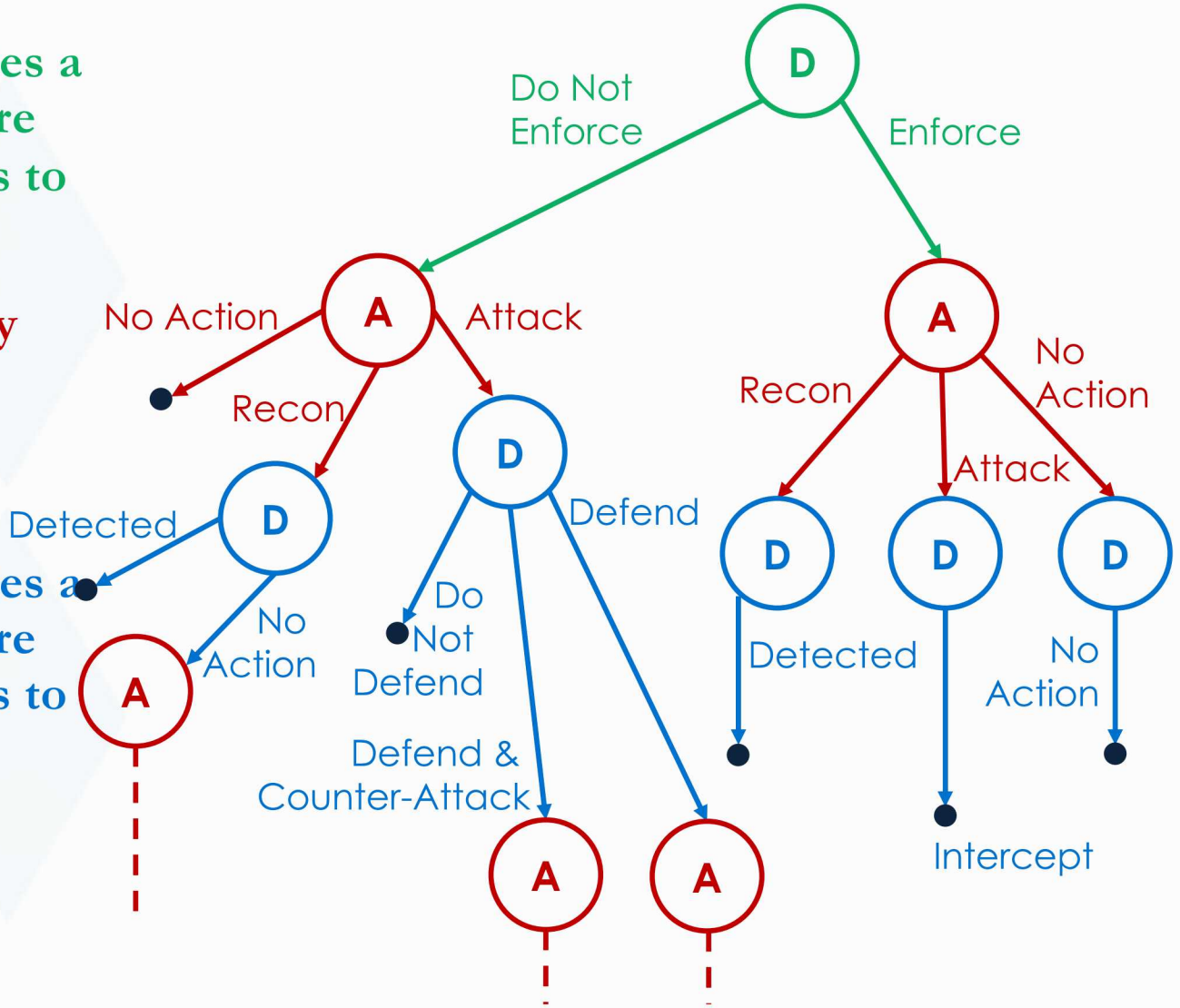
Defending Against: Empowered adversaries

Stackelberg Game:

Defender: An entity operates a cyber-enabled infrastructure and takes certain measures to defend it.

Attacker: A cyber adversary attacks the entity to cause service disruption and physical damage.

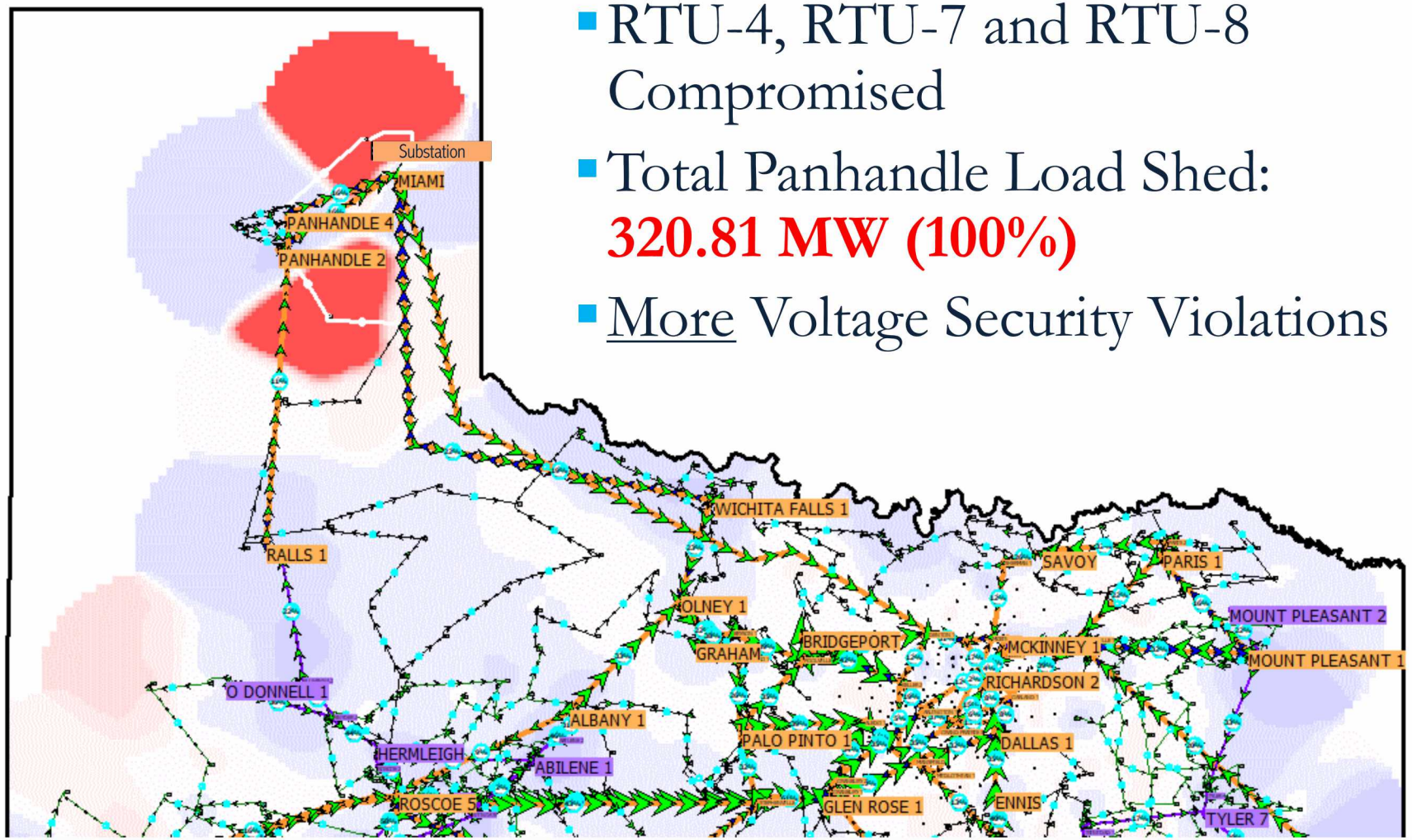
Defender: An entity operates a cyber-enabled infrastructure and takes certain measures to defend it.



EXEMPLAR: Worst-Case RTU Attack

Attack Budget of '3':

- RTU-4, RTU-7 and RTU-8 Compromised
- Total Panhandle Load Shed: **320.81 MW (100%)**
- More Voltage Security Violations



*Derived from synthetic data with no relation to actual grid: https://electricgrids.engr.tamu.edu/electric-grid-test-cases/activsg2000/

Conclusions

- Cyber experimentation is a crucial tool in the cyber security space.
- Emulation (abstract hardware/real software) provides predictive capability.
- Prediction should be support with confidence bounds to be used for high-consequence decisions.
- We need the ability to identify extreme events in systems.
- We face algorithmic challenges in
  - Dimension reduction for discontinuous systems
  - Ability to sample high-dimensional, categorical spaces
  - V&V for discrete systems
  - Threat Characterization
  - Glass-box models for cyber systems
  - Scalable solvers for design/interdiction problems
  - Scalable solvers stochastic design/interdiction problems
- We will be open to collaborations