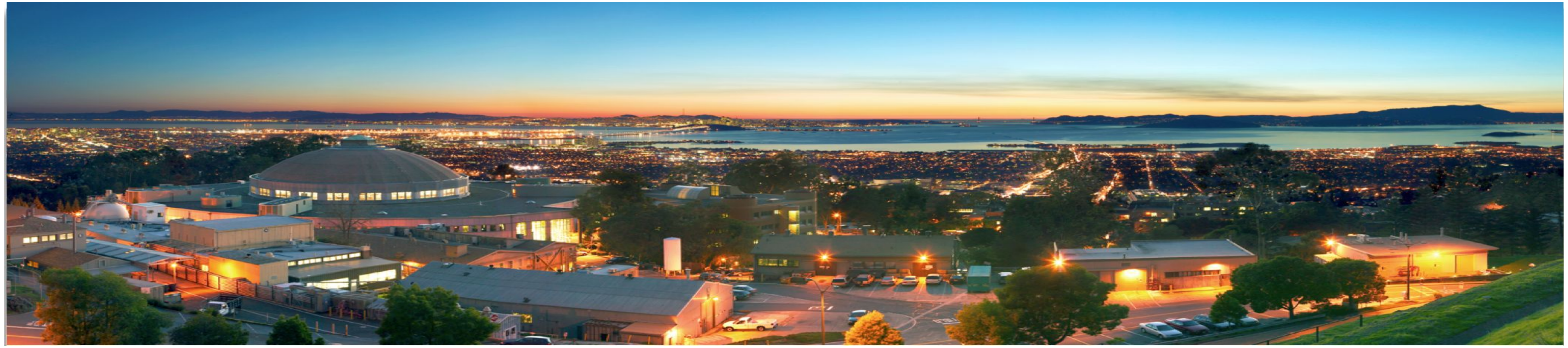


Cybersecurity via Inverter-Grid Automatic Reconfiguration (CIGAR)

End of Project Workshop

PIs: Sean Peisert & Daniel Arnold

Mar. 17, 2021

U.S. DEPARTMENT OF ENERGY

BERKELEY LAB
Lawrence Berkeley National Laboratory

Welcome!

- ***CIGAR Purpose:***
  - Develop AI methodology and tools allowing distribution grids to automatically reconfigure themselves to counteract cyberattacks that have affected distributed energy resources (e.g., solar photovoltaic systems).
- ***Workshop Goals:***
  - Present research methodology and developed software
  - Discuss and demonstrate results and outcomes of this project
- ***Workshop Participants:***
  - Project partners, sponsors & stakeholders, advisors, utility engineers

Agenda

- **10:00 - 10:30:** Opening Remarks & Project Overview (*Daniel Arnold & Sean Peisert - Lawrence Berkeley National Laboratory)*
- **10:30 - 10:50:** Reinforcement Learning & PyCIGAR Architecture (*Daniel Arnold - Lawrence Berkeley National Laboratory)*
- **10:50 - 11:15:** Simulation Experiments / Results *(Ciaran Roberts - Lawrence Berkeley National Laboratory)*
- **11:15 - 11:25:** (Break)
- **11:25 - 11:50:** Integration of PyCIGAR into NRECA Open Modeling Framework (OMF) *(David Pinney - National Rural Electric Cooperative Association)*
- **11:50 - 12:15:** Synthetic Data Generation and Linearized Power Flow Solver *(Ignacio Losada Carreno - Arizona State University)*
- **12:15 - 12:35:** Graph Convolutional Neural Networks and Siemens Technology Transfer *(Anton Kocheturov and Dmitriy Fradkin - Siemens Corporate Research)*
- **12:35 - 13:00:** Key Findings and Future Research Directions (*Daniel Arnold - Lawrence Berkeley National Laboratory)*

Overview of Cybersecurity Research at LBL

Host and network intrusion detection

Byzantine fault tolerance

Trusted HPC hardware/software co-design

Smart grid / industrial control system security

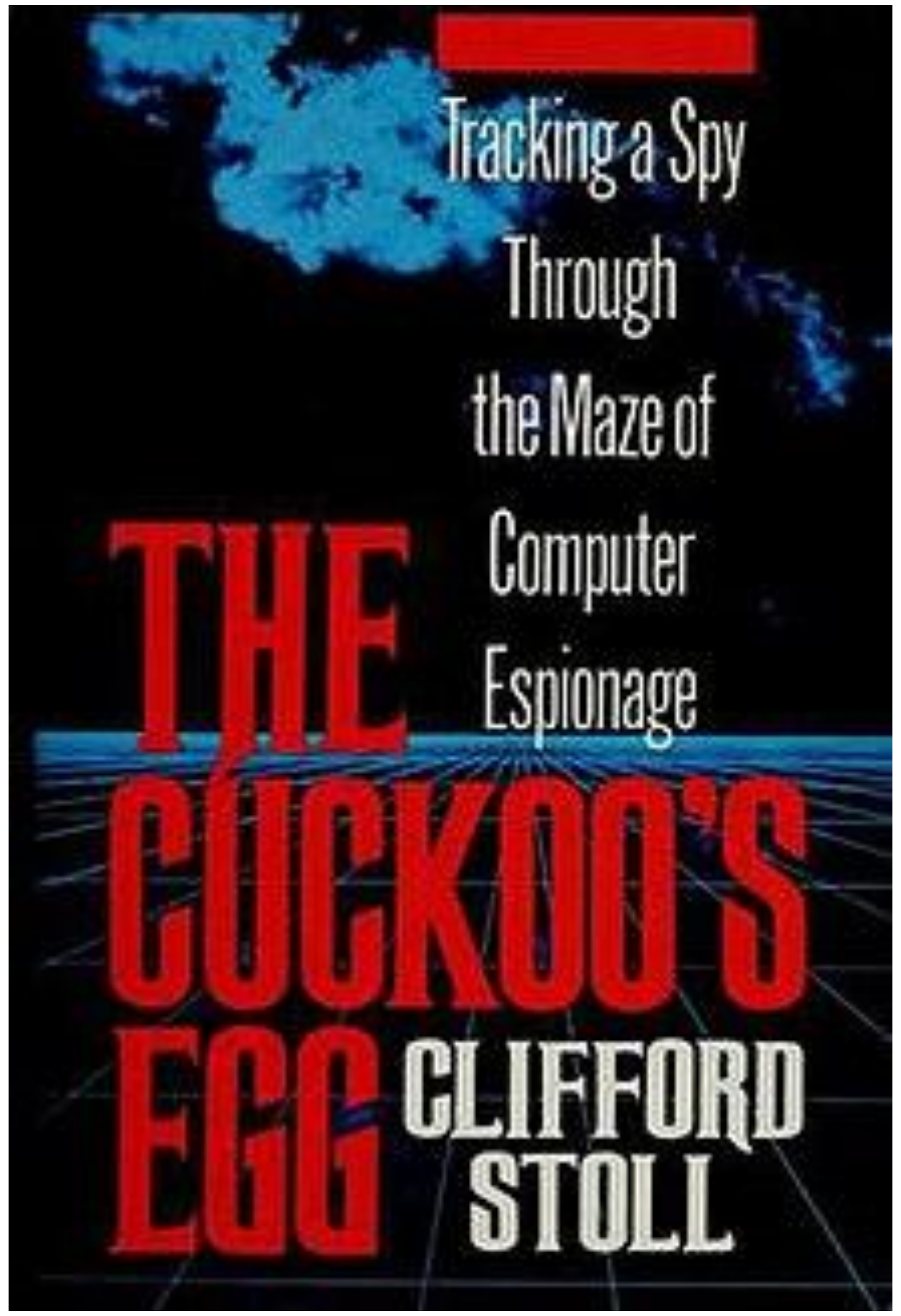
Data provenance

HPC program fingerprinting

ICS function fingerprinting

Data privacy

Network evolution modeling



Tracking a Spy Through the Maze of Computer Espionage

THE CUCKOO'S EGG

CLIFFORD STOLL

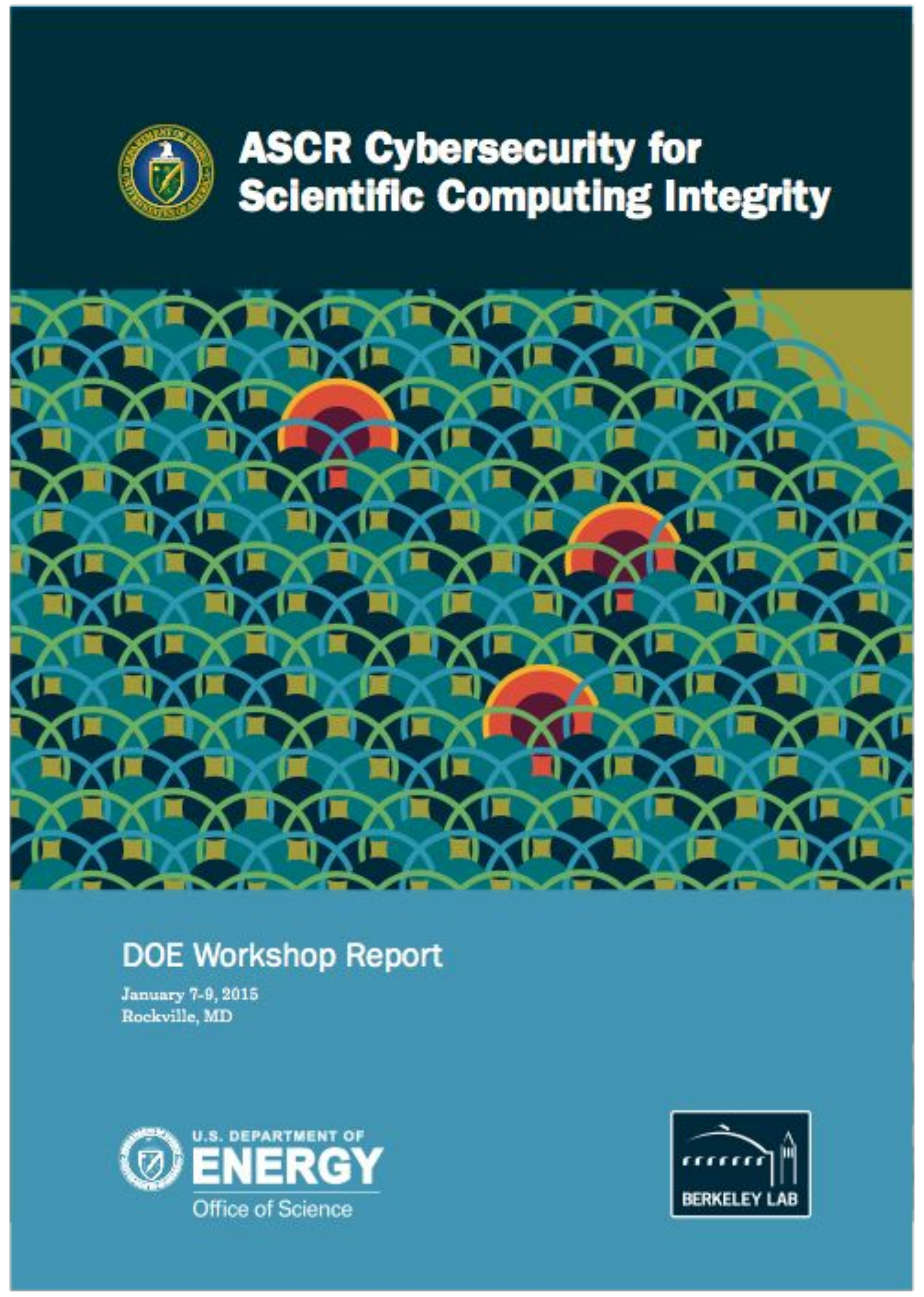
BRO NETWORK SECURITY MONITOR

zeek®

corelight

Two Key Themes (1)

- Cybersecurity R&D to enable scientific research
  - Particularly HPC systems (NERSC), and
  - High-throughput network backbones (ESnet)



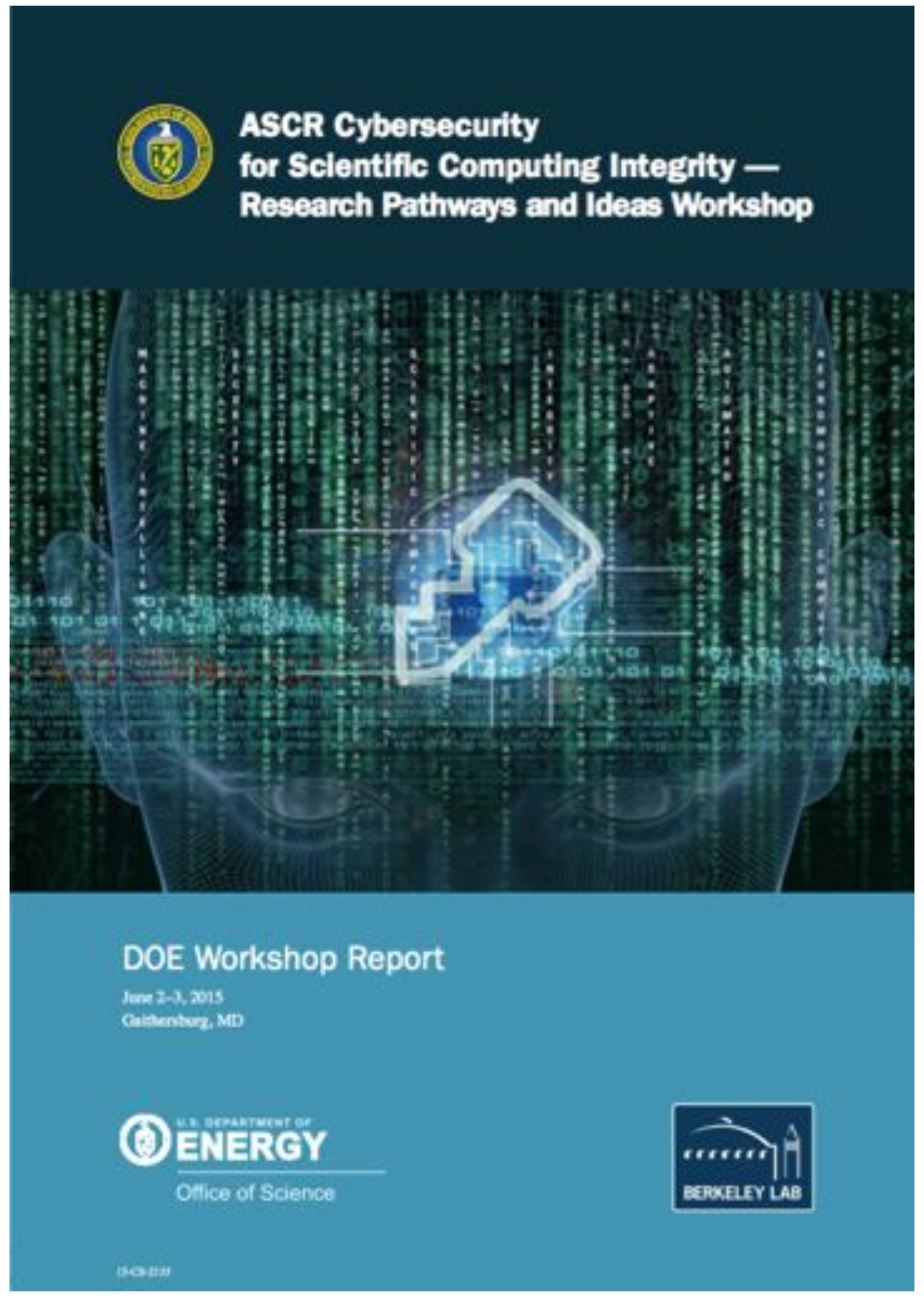
ASCR Cybersecurity for Scientific Computing Integrity

DOE Workshop Report

January 7-9, 2015
Rockville, MD

U.S. DEPARTMENT OF ENERGY
Office of Science

BERKELEY LAB



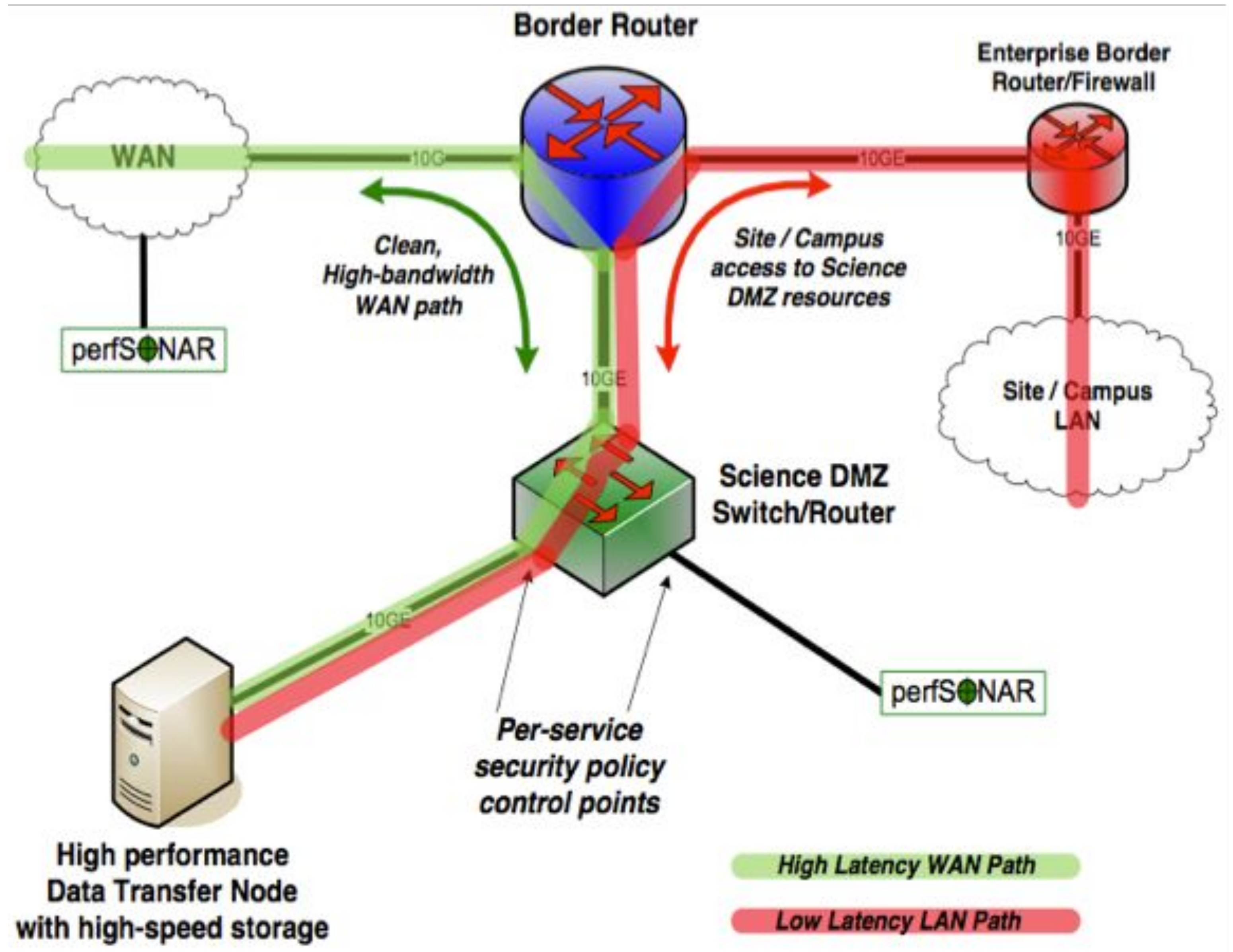
ASCR Cybersecurity for Scientific Computing Integrity — Research Pathways and Ideas Workshop

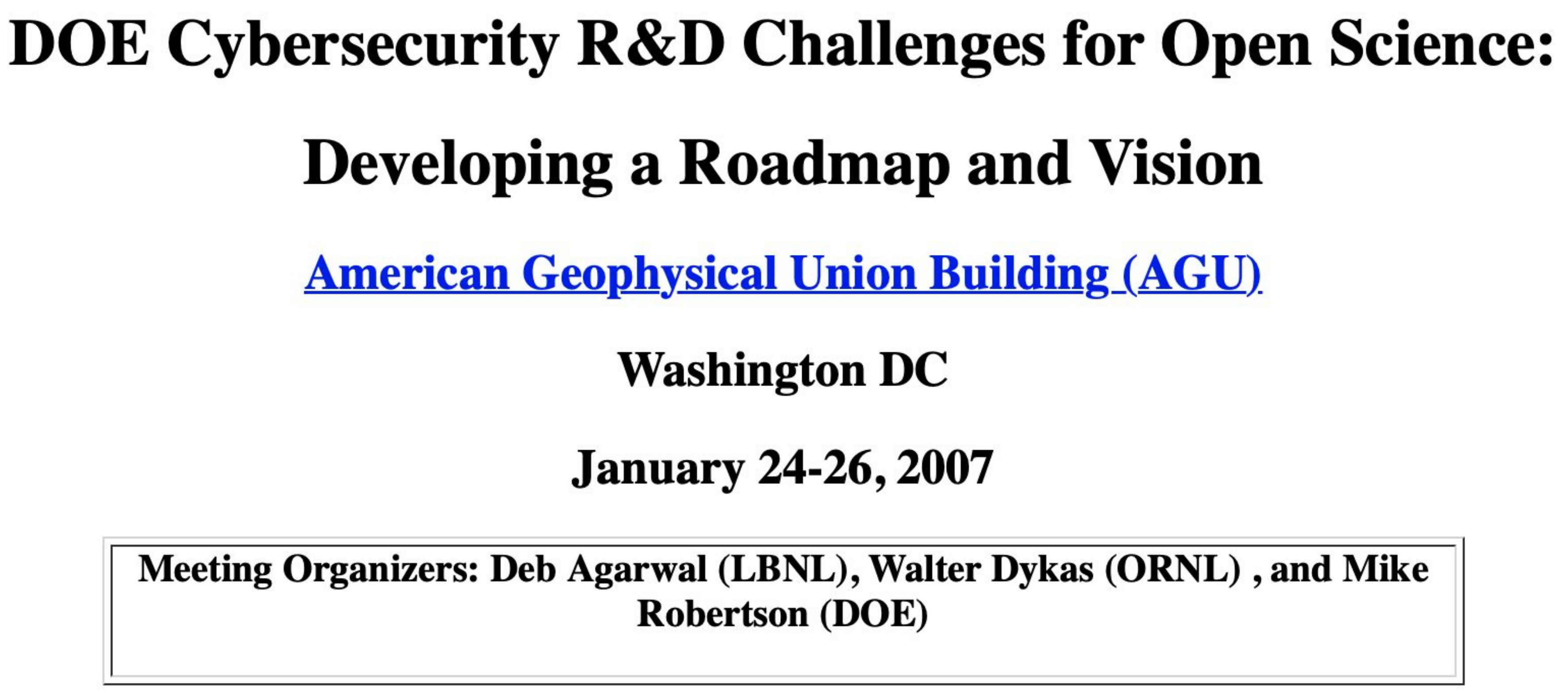
DOE Workshop Report

June 2-3, 2015
Gaithersburg, MD

U.S. DEPARTMENT OF ENERGY
Office of Science

BERKELEY LAB


Border Router
Enterprise Border Router/Firewall
WAN
10GE
10GE
10GE
10GE
10GE
Clean, High-bandwidth WAN path
Site / Campus access to Science DMZ resources
perfSONAR
Site / Campus LAN
Science DMZ Switch/Router
perfSONAR
Per-service security policy control points
High performance Data Transfer Node with high-speed storage
High Latency WAN Path
Low Latency LAN Path



DOE Cybersecurity R&D Challenges for Open Science:

Developing a Roadmap and Vision

American Geophysical Union Building (AGU)

Washington DC

January 24-26, 2007

Meeting Organizers: Deb Agarwal (LBNL), Walter Dykas (ORNL) , and Mike Robertson (DOE)

https://dst.lbl.gov/security/research/hpc-security/

Two Key Themes (2)

Cybersecurity R&D for securing the power grid

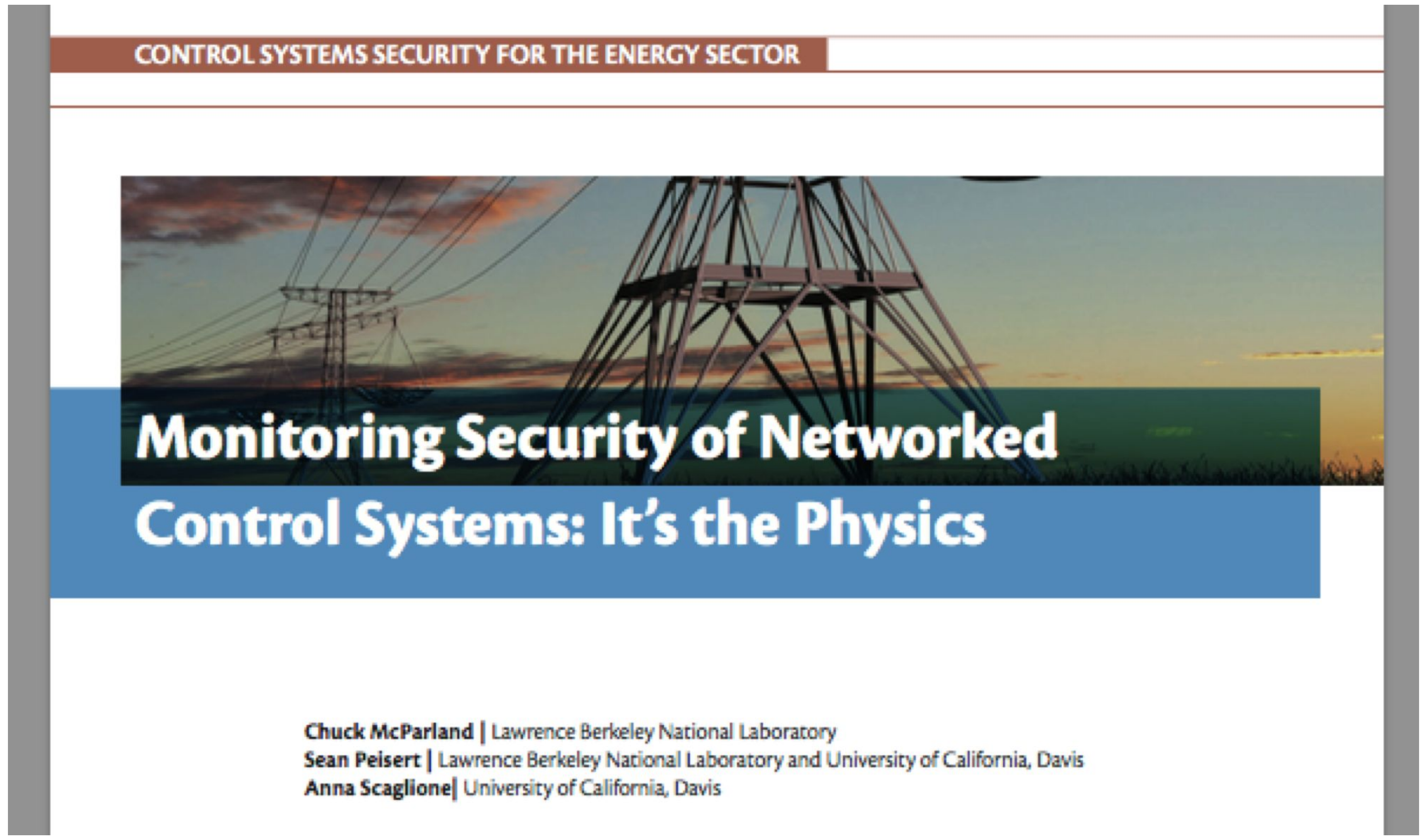
Cybersecurity R&D for CEDS since 2012

Past:

- Intrusion detection using physics and Zeek/Bro IDS
- Security monitoring using Distribution PMU data
- Integrated Multi Scale Machine Learning for the Power Grid (GMLC 1.4.9)
- Grid Threat Detection and Response with Data Analytics (GMLC 1.4.23)

Current:

- Privacy preserving security event detection
- Cybersecurity via Inverter-Grid Automatic Reconfiguration (“CIGAR”)
- Cybersecurity for for Distribution Energy Storage (“SPADES”)
- Byzantine Architecture for Bulk Power System Protective Relays (GMLC)



CONTROL SYSTEMS SECURITY FOR THE ENERGY SECTOR

Monitoring Security of Networked Control Systems: It’s the Physics

Chuck McParland | Lawrence Berkeley National Laboratory
Sean Peisert | Lawrence Berkeley National Laboratory and University of California, Davis
Anna Scaglione| University of California, Davis

https://dst.lbl.gov/security/research/ceds/

CIGAR Project Details

Performers:

BERKELEY LAB

Lead Institution

SIEMENS

NRECA
America's Electric Cooperatives

ASU
Arizona State University

PSL

Project Details:

- **Total Value of Award:** $2,500,000
- **Sponsor:** Cybersecurity for Energy Delivery Systems (CEDS) program, CESER Office
- **Period of performance:** 4/1/18 - 3/31/21
- **Project Tasks:**
  - Task 1: Feedback control modeling (completed 3/31/19)
  - Task 2: AI algorithm and prototype software development (completed 3/31/2020)
  - Task 3: Integration of AI algorithm into Open Modeling Framework (OMF) (completed 3/01/2021)

CIGAR Project Details

Performers:

Lead Institution

Roles:

- **LBNL:** Project management, feedback control modeling, AI algorithm development, software design, OMF integration
- **Siemens:** AI algorithm development
- **ASU:** Feedback control modeling, software design
- **NRECA:** OMF integration, support to all other project tasks
- **PSL:** Project advisor (PSL left project in 2019 following acquisition)

CIGAR Objectives

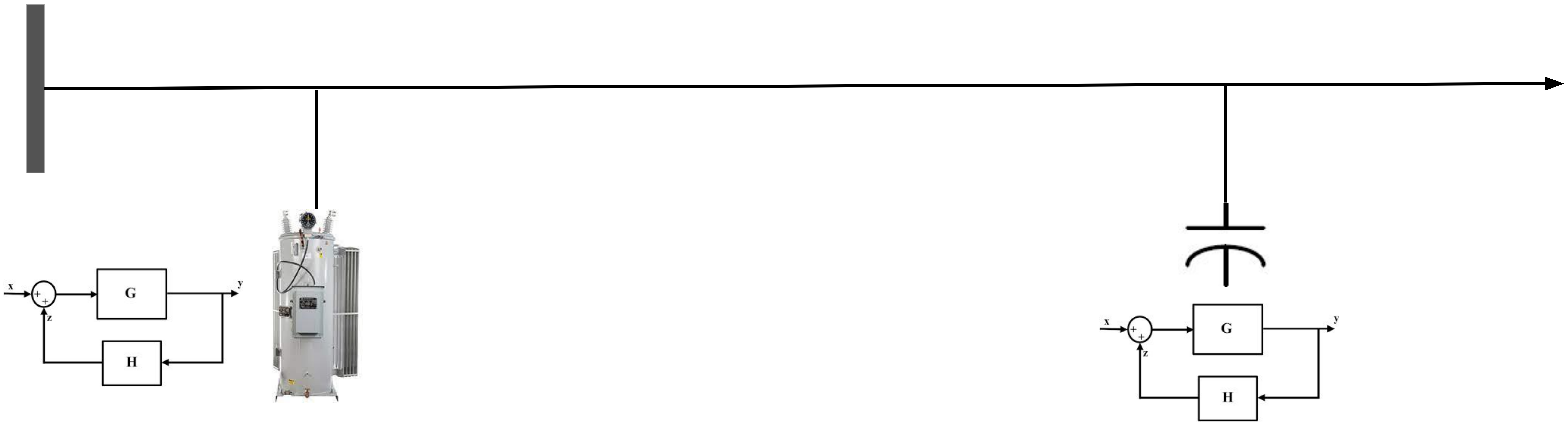
1. Develop the capability to train Reinforcement Learning (RL) algorithms (agents) to control the behavior of electric power distribution systems with high penetrations of solar photovoltaic (PV) systems
    a. Necessitates the creation of a software framework to merge grid simulation tools, dynamic models of PV systems, and RL training tools
2. Train RL agents to control PV systems to mitigate the effect of cyber attacks on the distribution grid
3. Integrate RL algorithms into an open source platform to facilitate utility access

CIGAR Benefits

- CIGAR allows the development of controllers for *non-compromised* solar inverters to mitigate the destabilizing effects of compromised units. Utilities can leverage existing assets in their systems to promote cyber resiliency and reduce the severity of attacks in their systems.
- The CIGAR framework can be extended to optimize the behavior of all types of Distributed Energy Resources (e.g. battery storage systems and EVs) holistically, leveraging the unique characteristics of each device class to minimize the impact of cyber attacks.
  - The tools developed for CIGAR are able to find controllers that take into account other dynamics in the system (e.g., regulator action)
- Integration of the reinforcement learning agent into the NRECA Open Modeling Framework allows utilities to upload system models for agent training and simulation
  - Analysis could lead to system hardening on network specific basis

Increasing Grid Complexity

In the past, relatively few control systems acting in a distribution grid

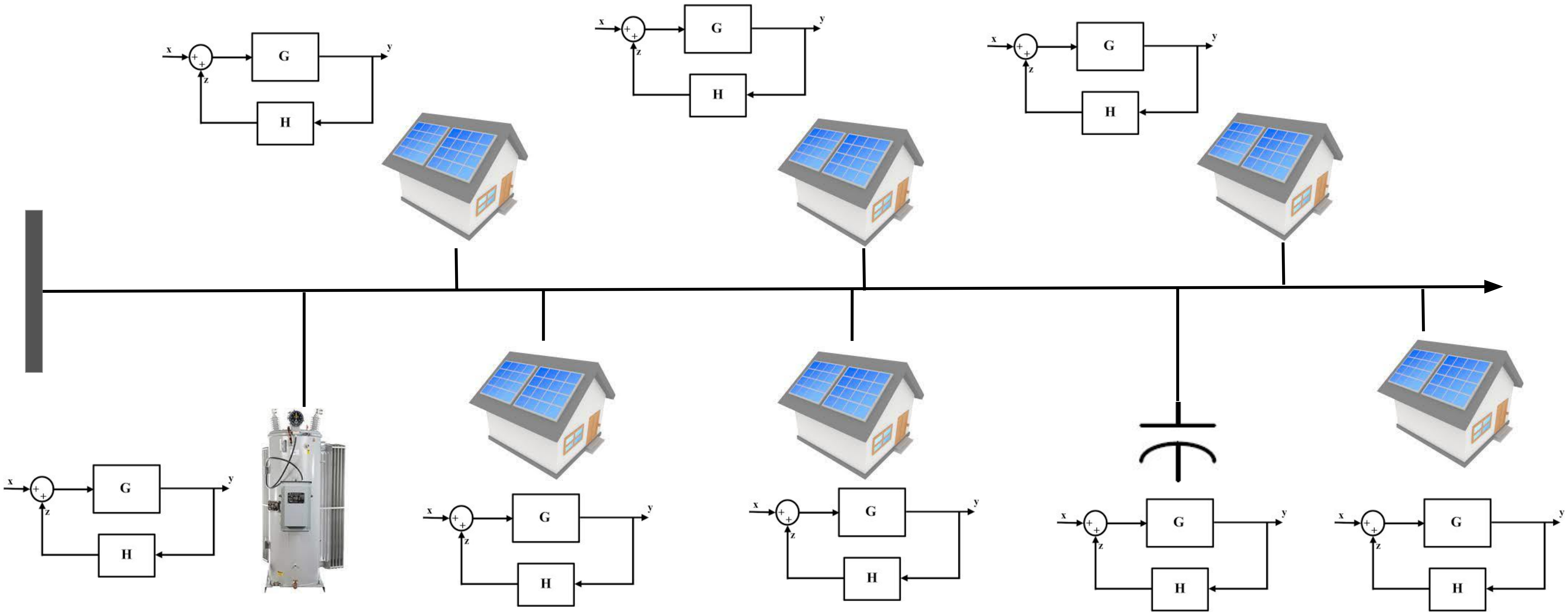


voltage regulator

cap. bank

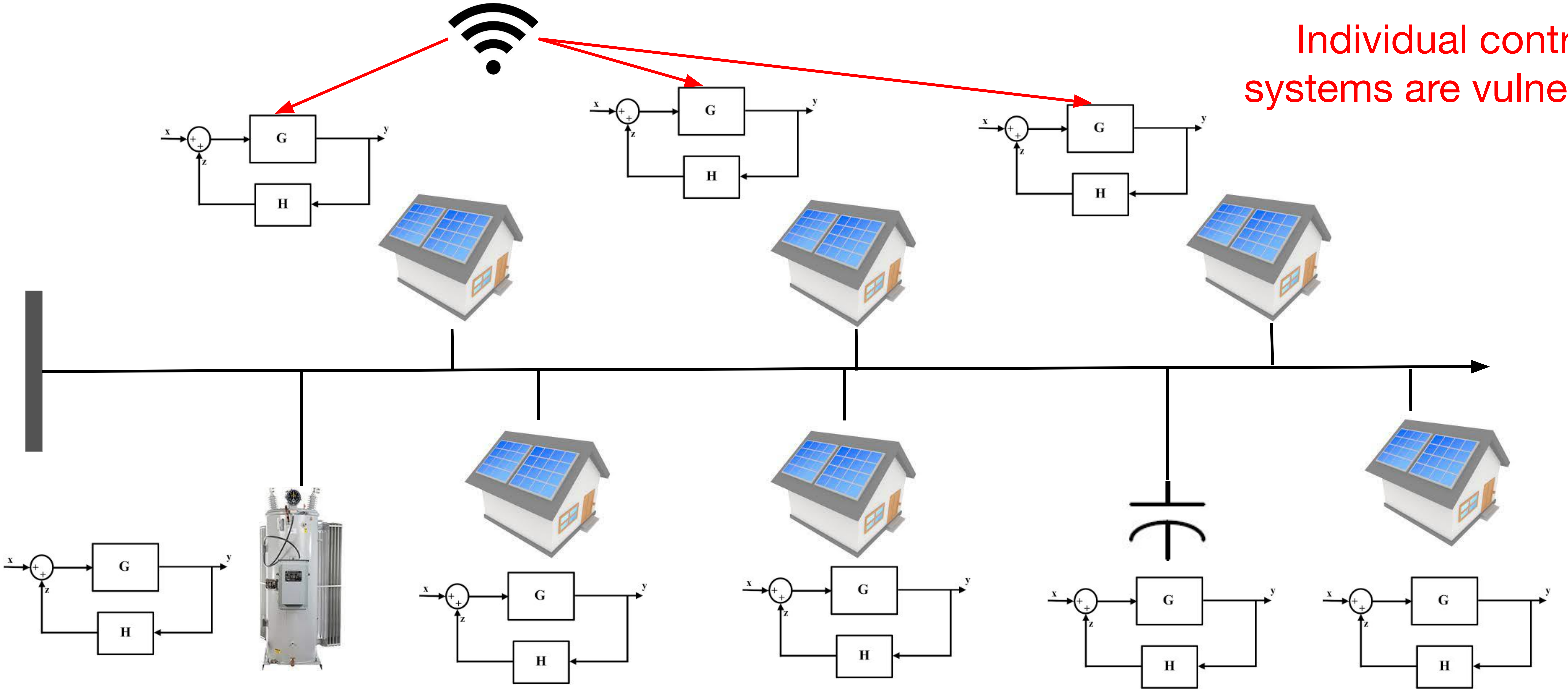
More Autonomous Control

Distributed generation introduces more feedback loops



Controls not holistically optimized

More Autonomous Control



Individual control systems are vulnerable

DER Control IoT Exposure

Control Parameters are Remotely Configurable

“800,000 Microinverters Remotely Retrofitted on Oahu—in One Day”

“…Enphase used built-in communications links to upgrade the grid-stabilizing capacity of four-fifths of Hawaii's rooftop solar systems”

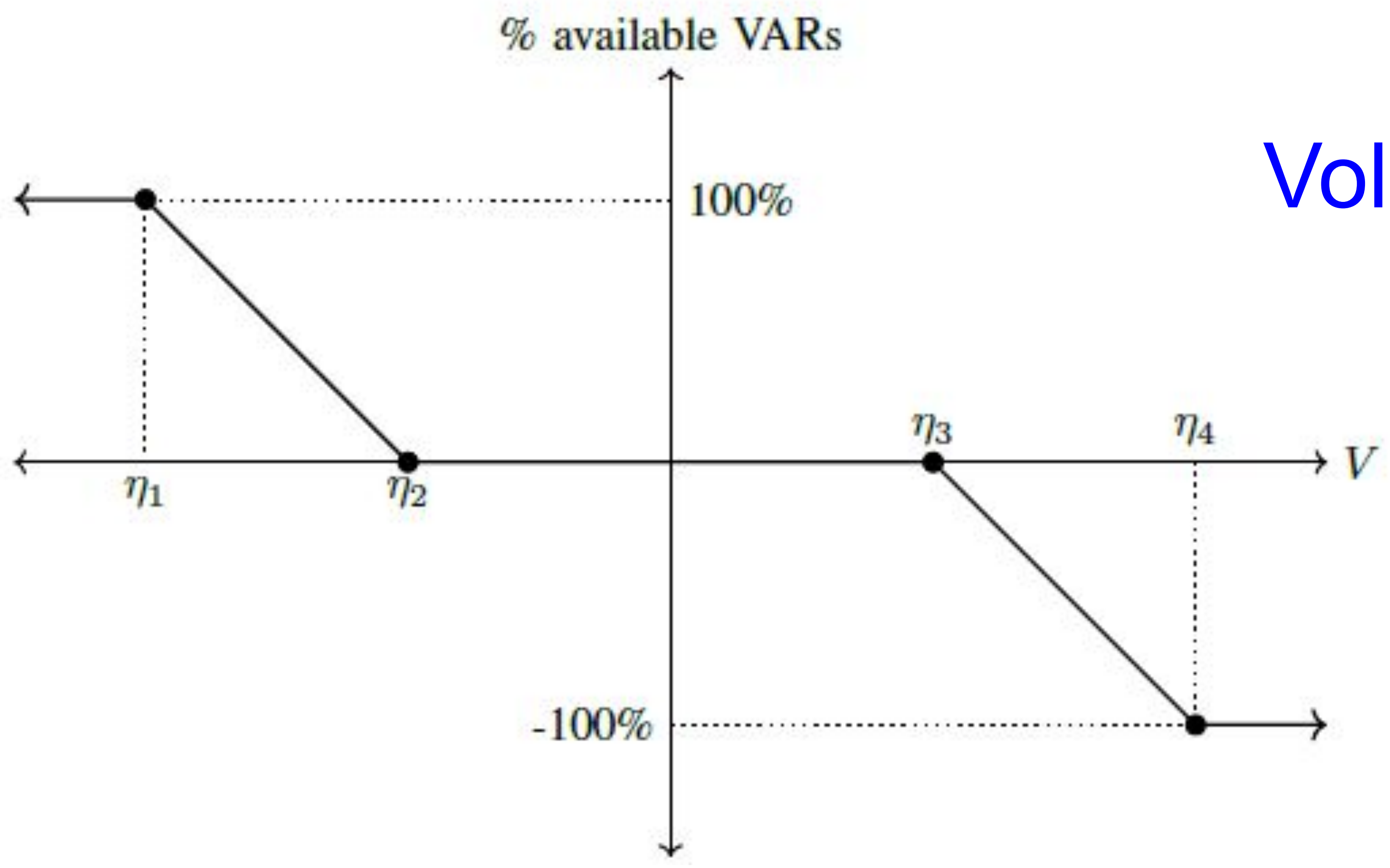
If compromised, what would happen?

How can we defend against this?

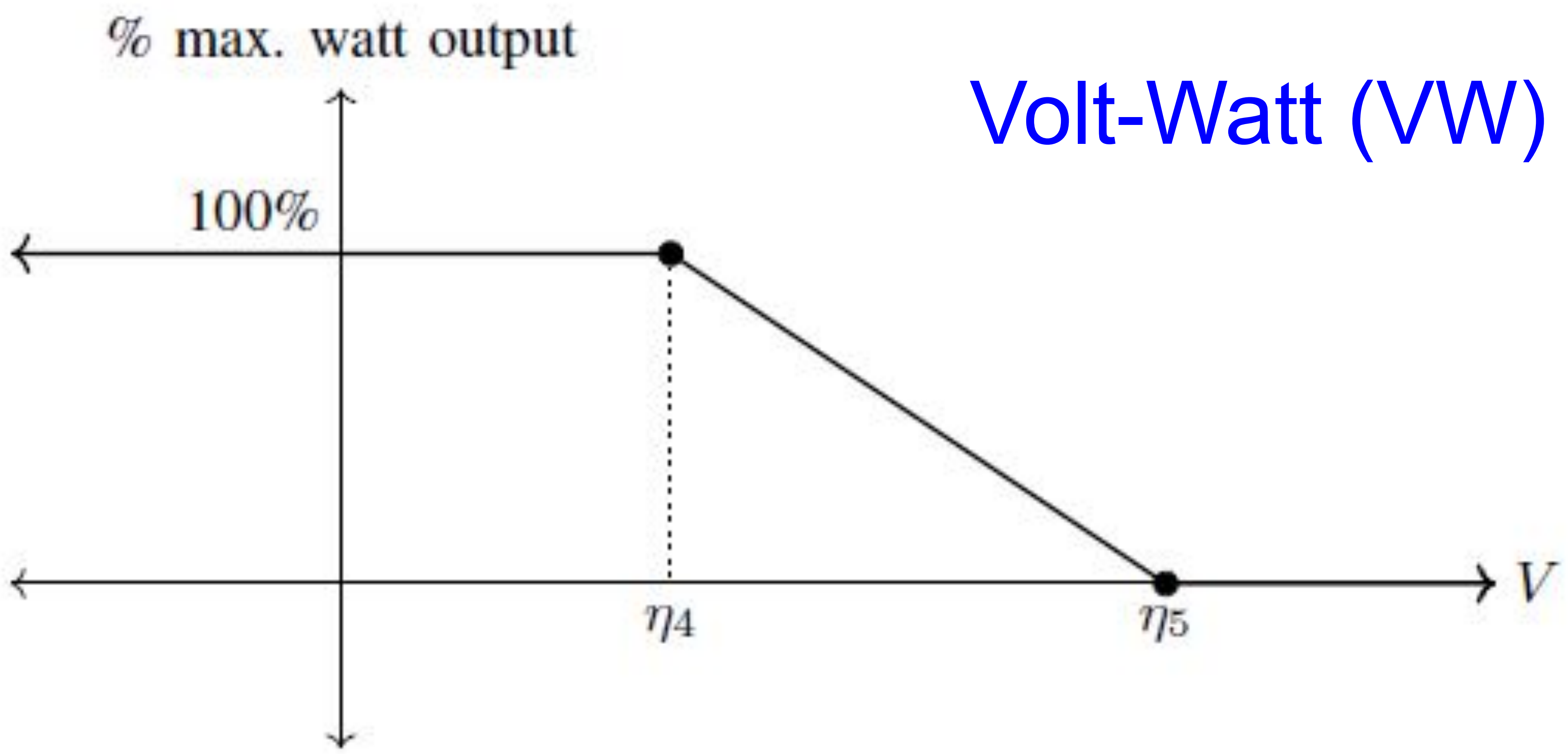
https://spectrum.ieee.org/energywise/green-tech/solar/in-one-day-800000-microinverters-remotely-retrofitted-on-oahu

DER Standardized Control (IEEE 1547)

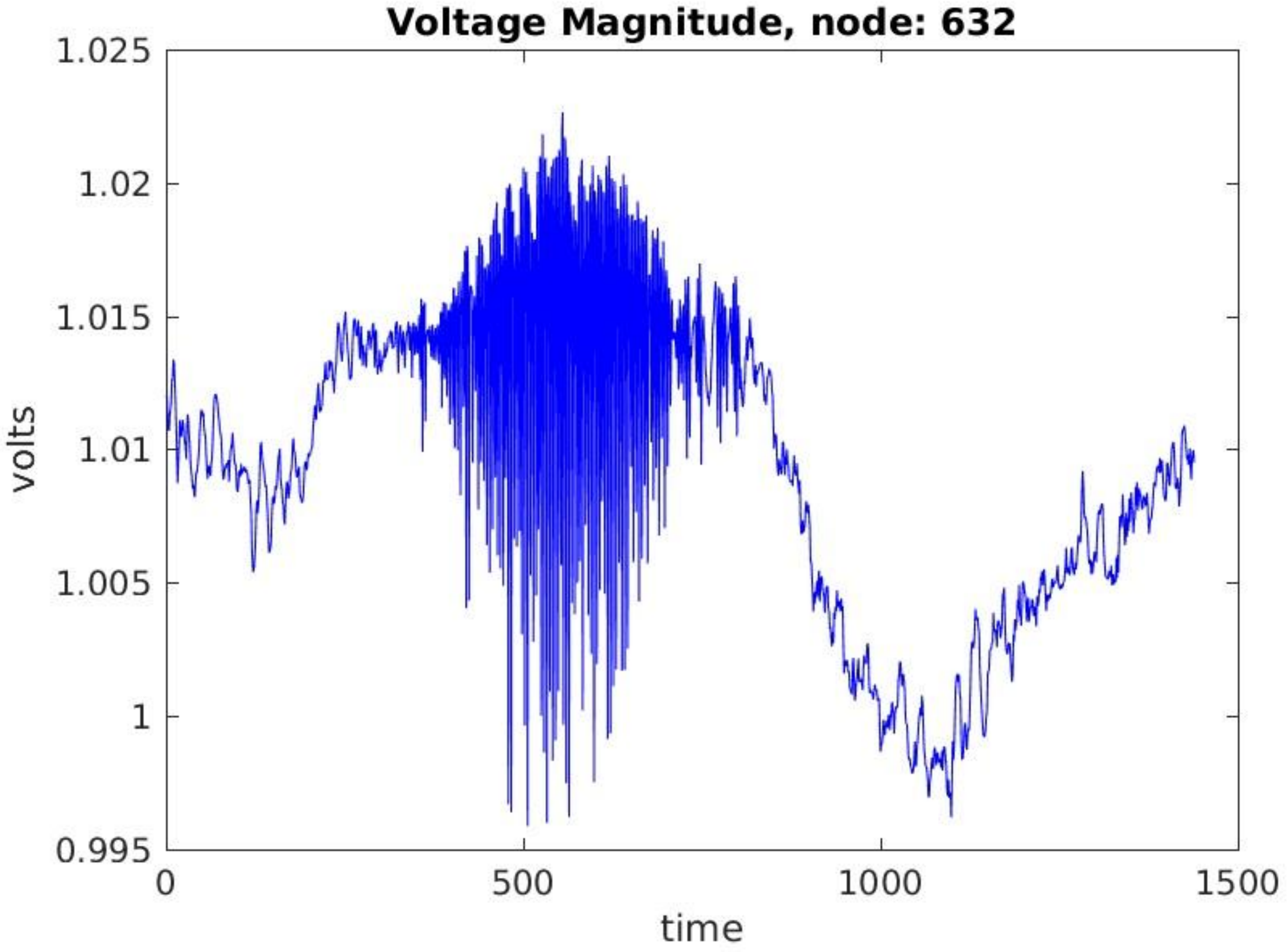
Cyberattack on DER Smart Inverter Settings



Volt-Var (VV)



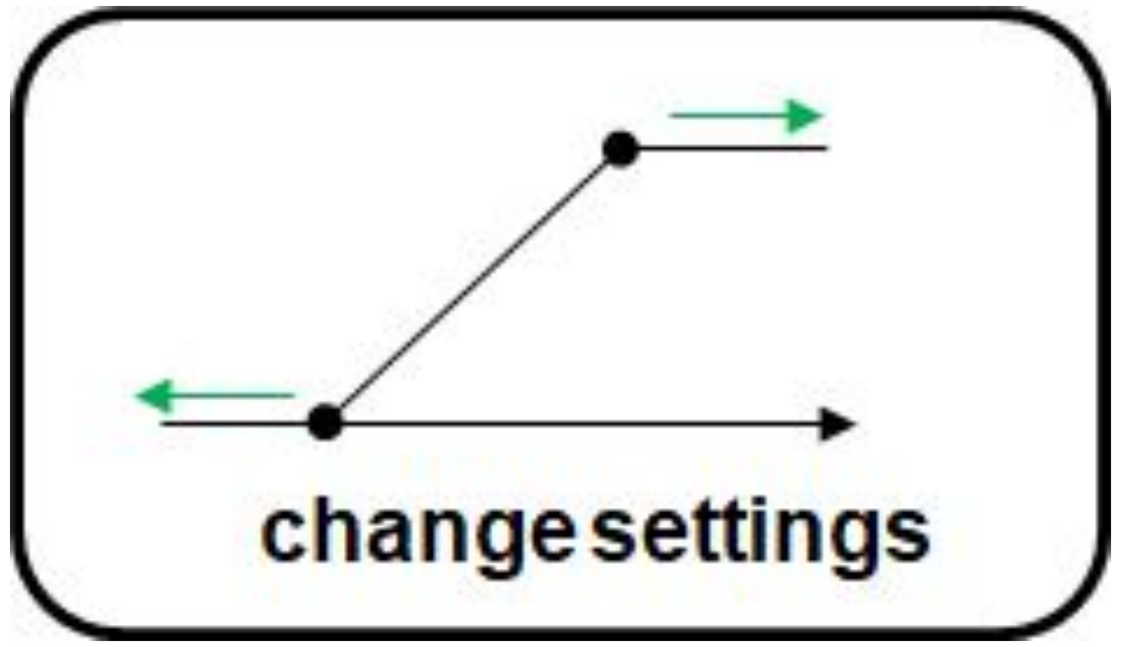
Volt-Watt (VW)

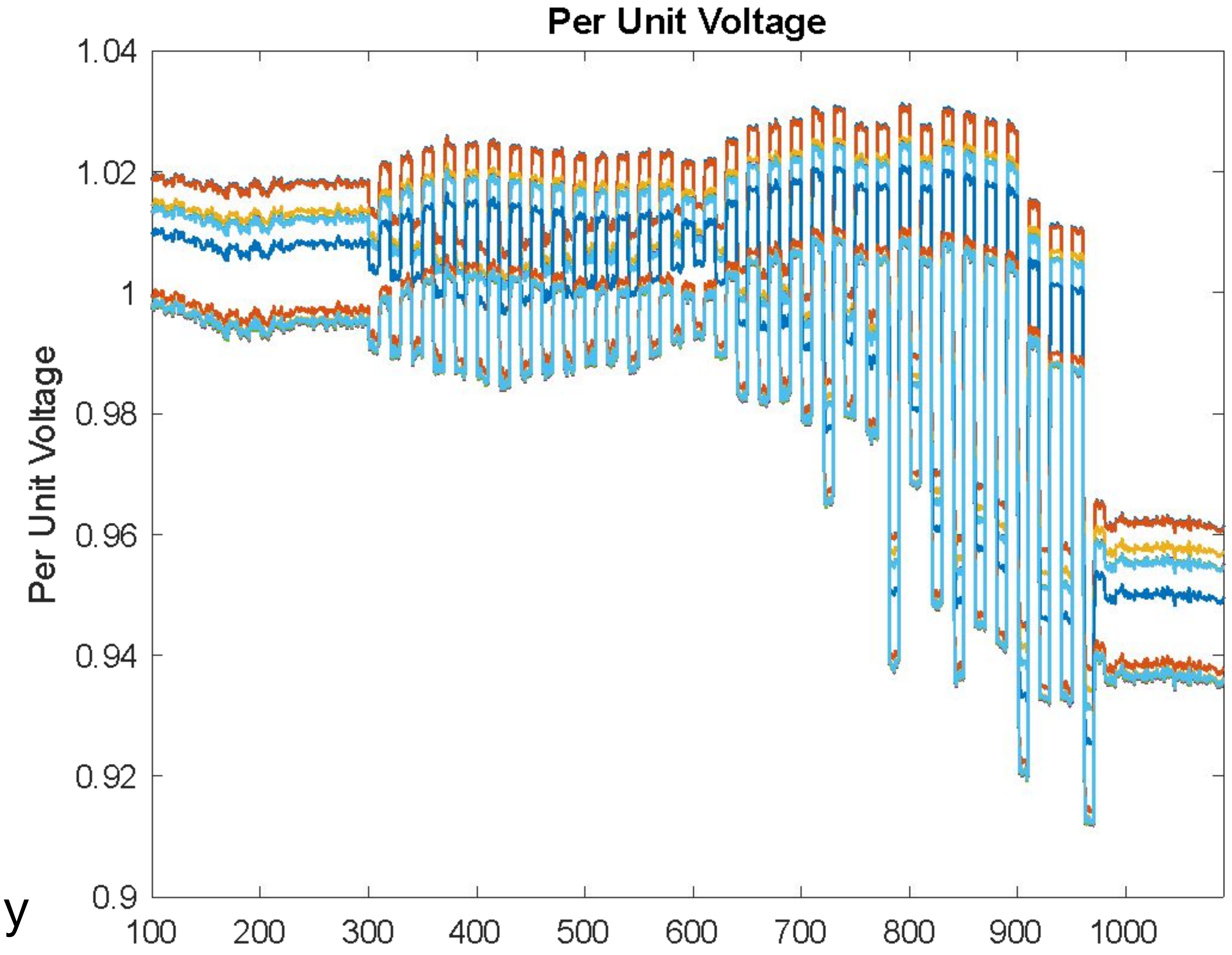


Simulation of improperly tuned settings that cause instabilities

CIGAR Solution

Reconfigure Control Parameters in Non-Compromised Units

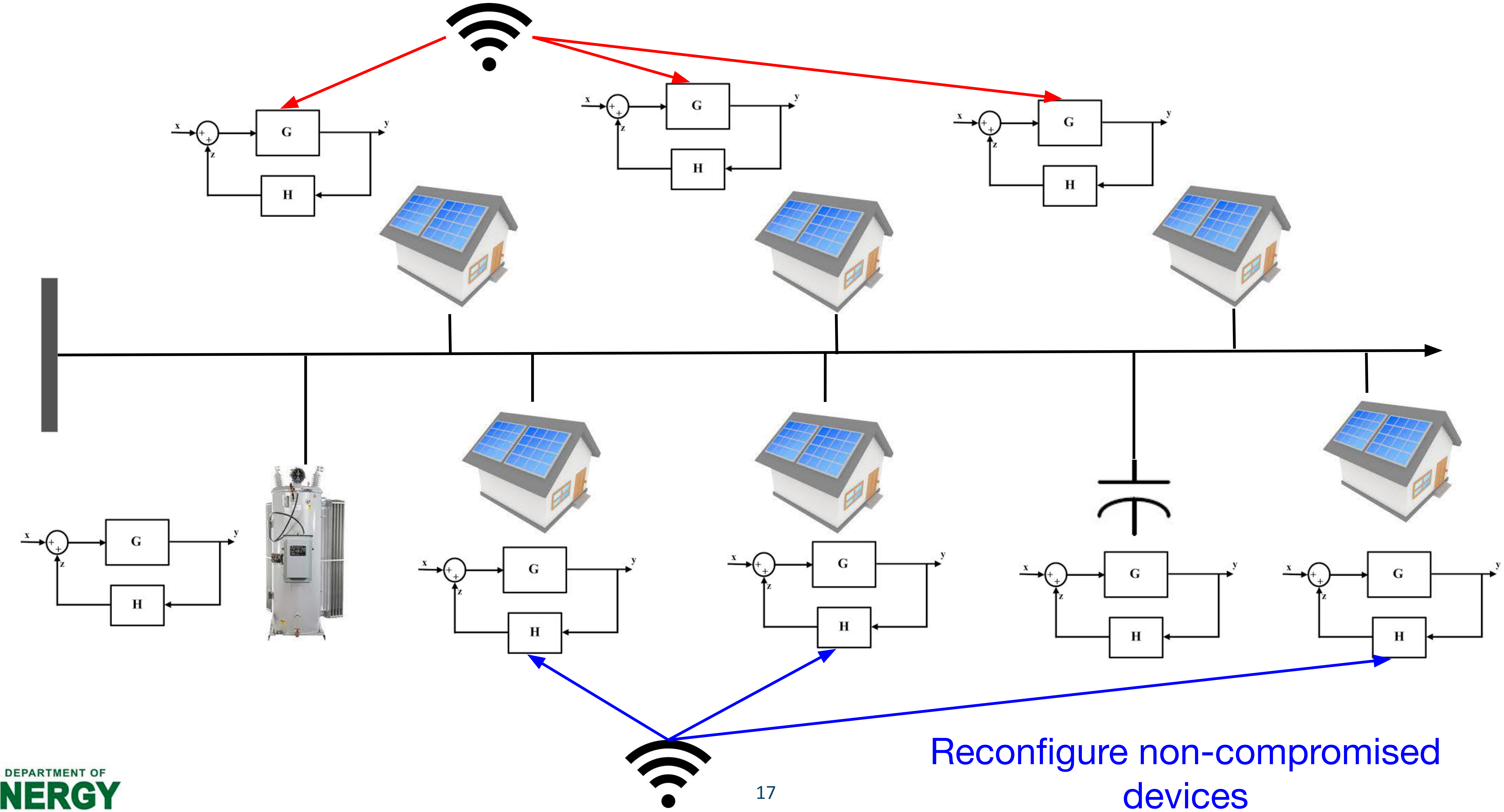




Control Paradigms:

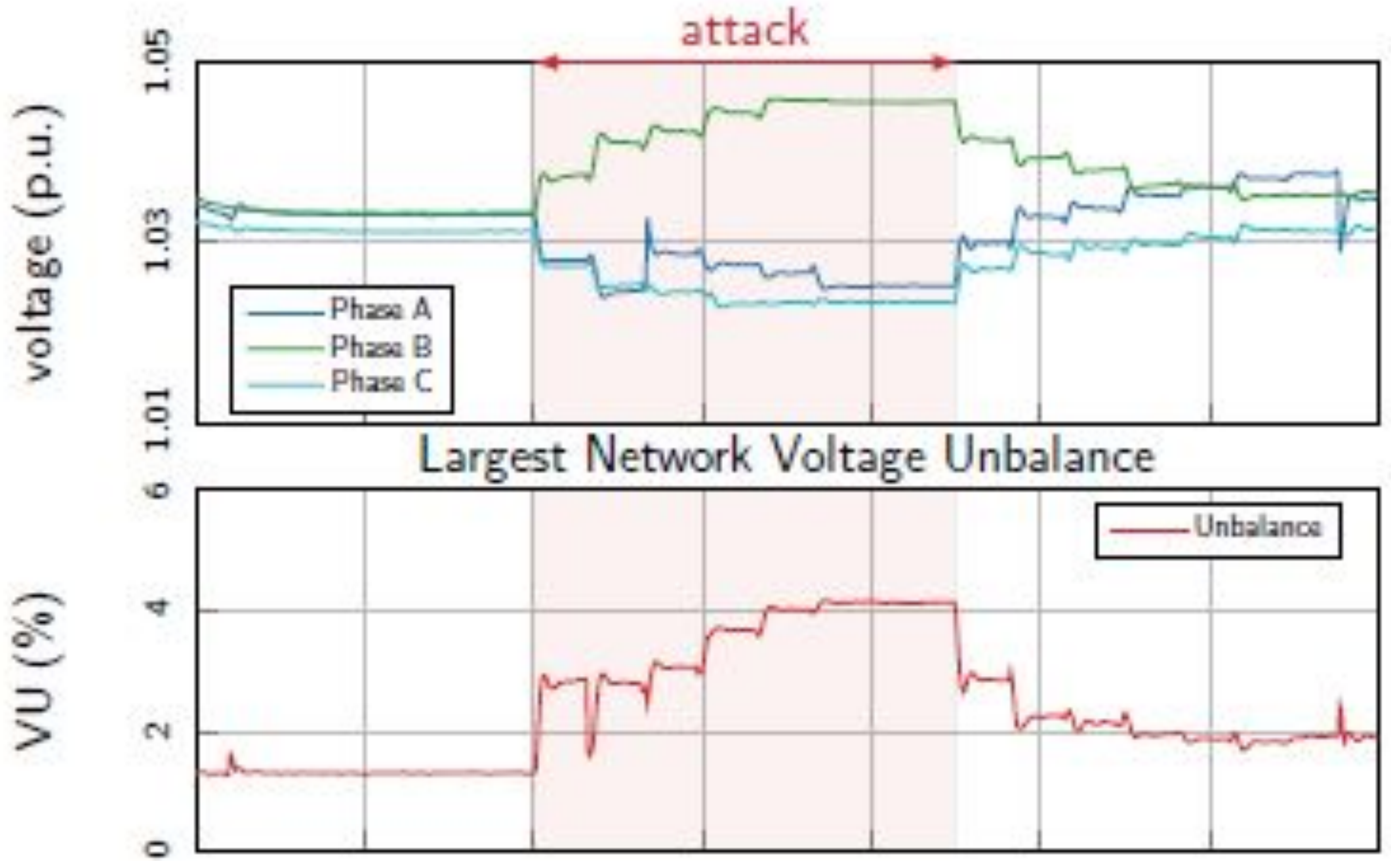
- **Centralized:** pre-determine new control curves for all non-compromised DER (all devices receive same settings)
- **Distributed:** algorithms are designed to be embedded directly in devices (devices determine settings independently based on local grid conditions)

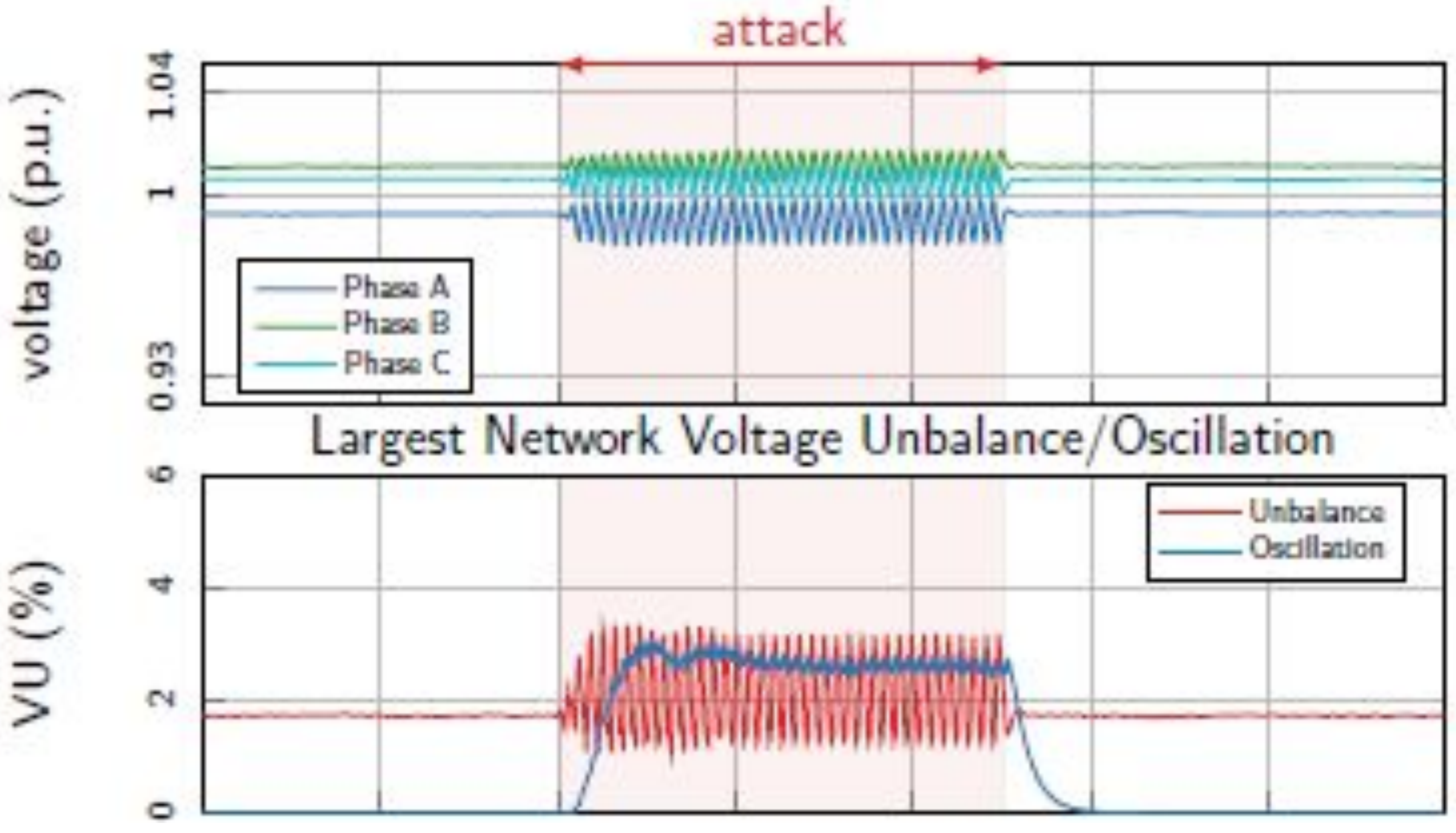
Reconfigure Non-Compromised Devices



Reconfigure non-compromised devices

Types of Attacks Explored



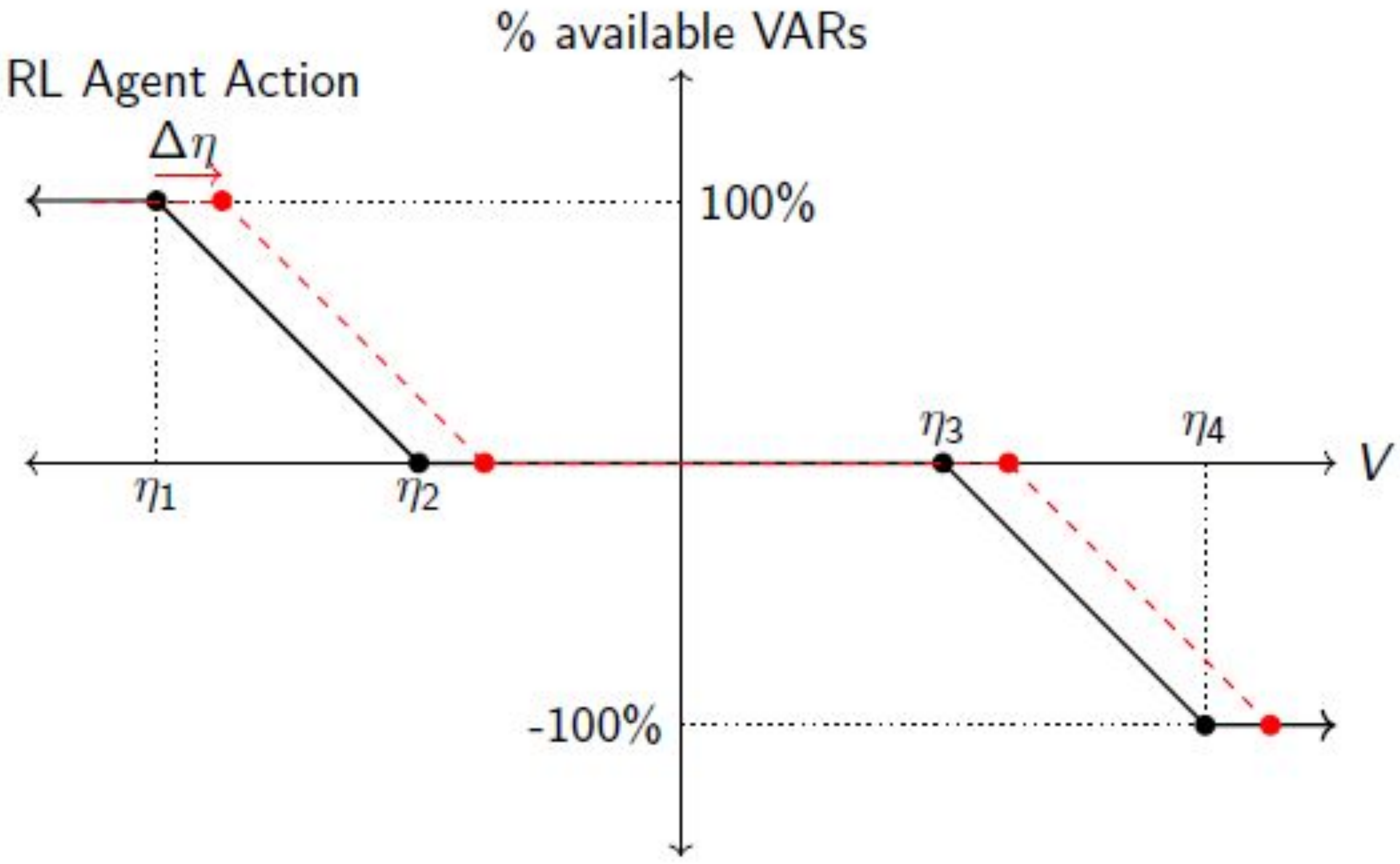


Attacker designs smart inverter Volt-VAR & Volt-Watt settings to create large voltage imbalances

Attacker designs smart inverter Volt-VAR & Volt-Watt settings to create oscillations in the system

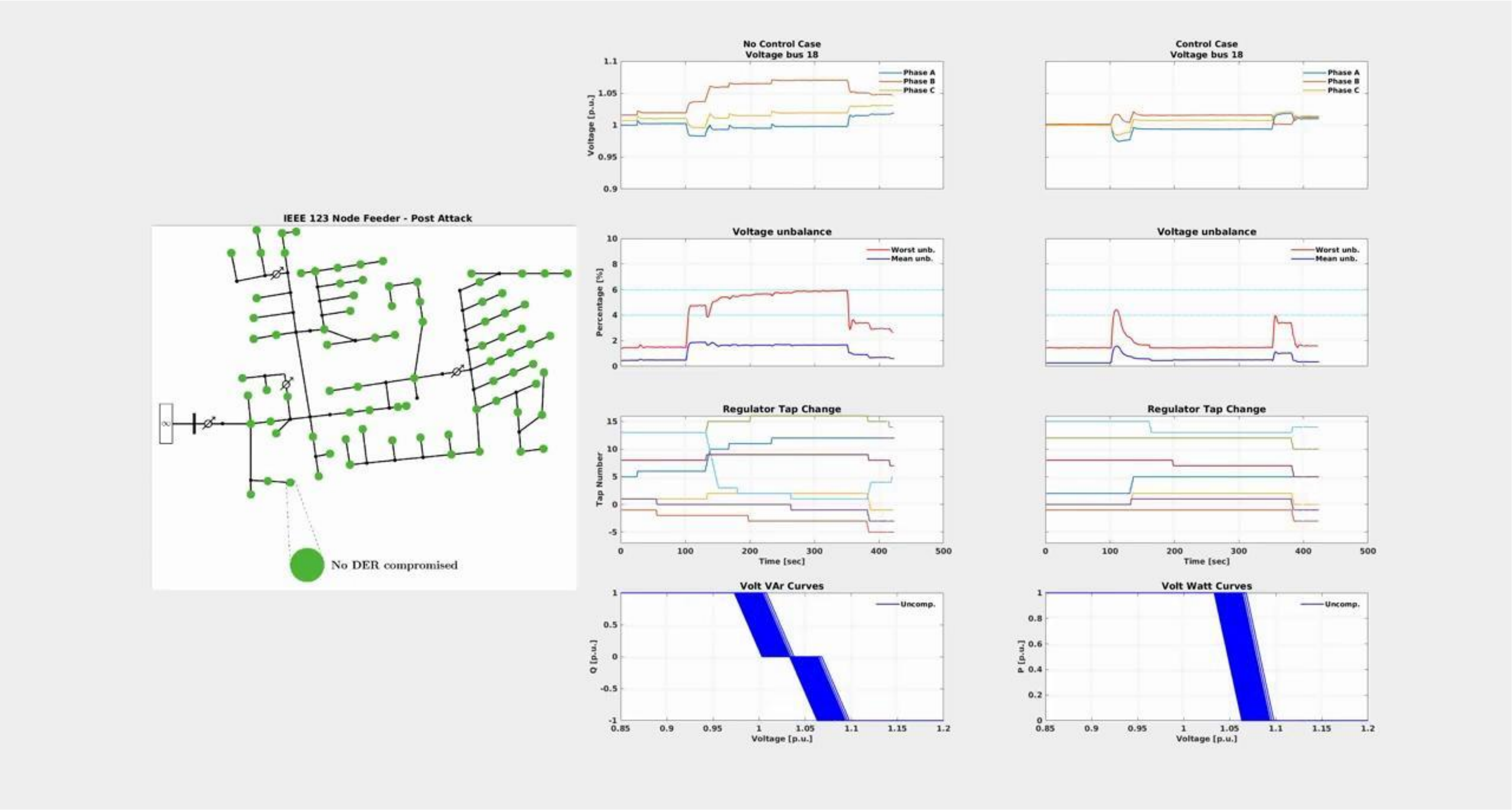
Control Implementation

- Reinforcement Learning action is the deviation from default VV/VW parameterization
- Translating the curves was found to yield superior results during training
- The agent learns to indirectly control reactive/real power injection/consumption



RL agent action: $a_t = \Delta\eta$

Videos



IEEE 123 Node Feeder - Post Attack
No DER compromised
No Control Case
Voltage bus 18
Control Case
Voltage bus 18
Voltage [p.u.]
Phase A
Phase B
Phase C
Voltage unbalance
Percentage [%]
Worst unb.
Mean unb.
Regulator Tap Change
Tap Number
Time [sec]
Volt VAr Curves
Q [p.u.]
Volt Watt Curves
P [p.u.]
Voltage [p.u.]
Uncomp.

Upcoming Presentations

- ***Description of RL & Software Architecture***
- ***Review of Simulation Experiments / Results***
- ***Demonstration of RL Agents in Open Modeling Framework***
- ***Discussion of Synthetic Data Generation Tool and Linearized Power Flow Models***
  - *Synthetic Data Generation: needed to populate realistic data for agent training*
  - *Linearized Power Flow: needed in case off-the-shelf tools prevent training on large networks*
- ***Discussion of Graph Convolutional Networks (GCN) and Addt'l Tech. Transfer***
  - *GCN has the potential to allow training of an agent that is viable for different networks*
- ***Discussion of Key Findings and Future Research Directions***

Questions/Discussion