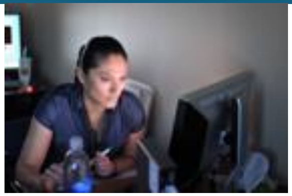
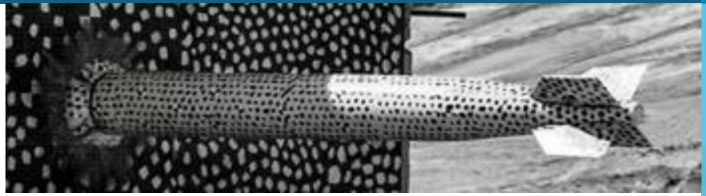
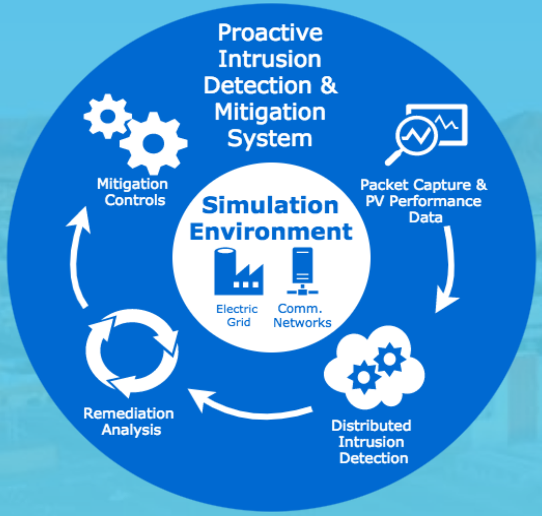
Securing Inverter Communication: Proactive Intrusion Detection and Mitigation System Sensor to Tap, Analyze, and Act



PRESENTED BY

Shamina Hossain-McKenzie (PI)
shossai@sandia.gov

SNL Team Members: Christine Lai, Nick Jacobs, Adrian Chavez, C. Birk Jones, Jay Johnson, and Adam Summers

Project Partners: Electric Power Research Institute (EPRI) and OPAL-RT

This material is based upon work supported by the U.S. Department of Energy's Office of Energy Efficiency and Renewable Energy (EERE) under Solar Energy Technologies Office (SETO) Agreement Number 34234.

SAND2019-5296 PE

Motivation: Role of Smart Inverters in the Future Grid

Future Vision

- High penetrations of variable PV; automated, controllable DERs to maintain stability
- Remote-access functionalities including advanced comm., access interfaces, and third-party software
- **Comm. network and interfaces will be equipped with encryption, firewalls, IDSs, and mitigation control defenses**

Present State

- Unsecure communication networks
- Non-standardized cybersecurity practices in industry
- Limited PV system cybersecurity
  - IDS are not required for DER communication or utility networks

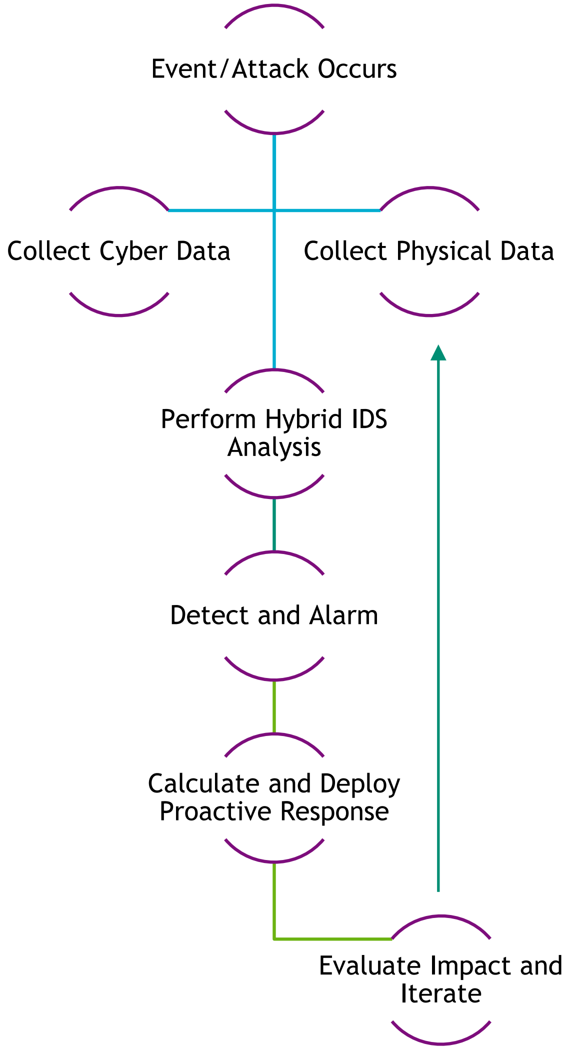
Threats and Vulnerabilities

- Breaches in network security and weak access control on inverters
  - 2017 SMA Solar Technology AG's inverter software flaws: 21 vulnerabilities
  - 2015 Ukrainian power grid cyber attack: malicious firmware updates

Solution Need and Importance

- Due to grid-support needs and rapid transition from passive to highly active DER devices, security must be prioritized
- Smart inverters play critical role in the grid but are vulnerable
- Need to detect AND respond

Project Objectives



Proposed Solution — PIDMS

- This project will secure PV inverter communication in DER systems by developing a bump-in-the-wire (BITW) proactive intrusion detection system and mitigation system (PIDMS) sensor

Unique Capabilities — Detect and Mitigate

- The PIDMS sensor will leverage cyber-physical data and operate at the grid-edge to achieve distributed, device-level defense
- It will not only detect and alarm adversarial activity, but also take preventative and/or mitigative actions automatically in response

High-fidelity validation — Unique Testing Environment

- Build and test the PIDMS in a unique simulation environment that combines the grid components with advanced communication networks

Project Objectives

Create High-Fidelity Emulation Environment

Using Sandia's virtual machine manager tool, minimega

EPRI DER Simulator with comm. upgrades and full suite of IEEE 1547 functions

OPAL-RT with ePhasorSim and updated comm. drivers

Build BITW Data Collection Sensor

Create packet capture tool functionality to capture and collect cyber-physical data

Build lightweight and reliable data collection sensor with low dropout rate

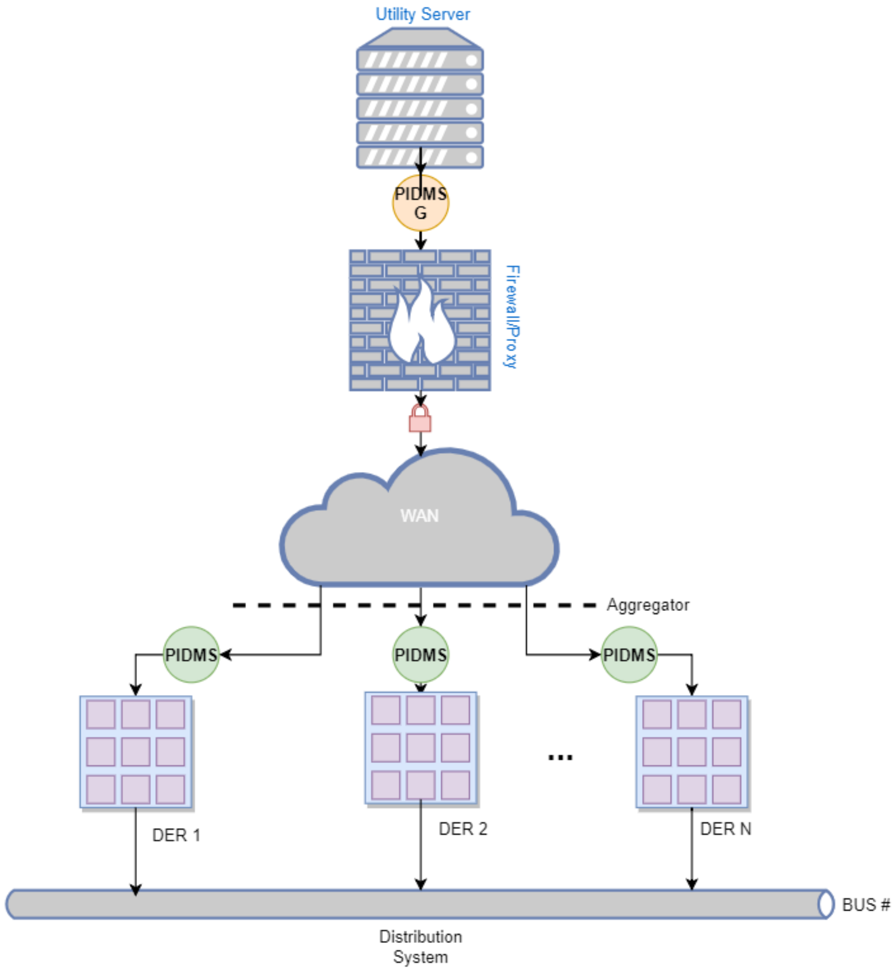
Create subscriber/publisher communication platform and framework for peer-to-peer communication between sensors

Develop PIDMS Analysis and Control Methodology

Develop hybrid approach for intrusion detection that combines signature- and behavioral-based IDS methods and processes cyber-physical data

Develop remedial action strategies to prevent detected events or lessen system impact

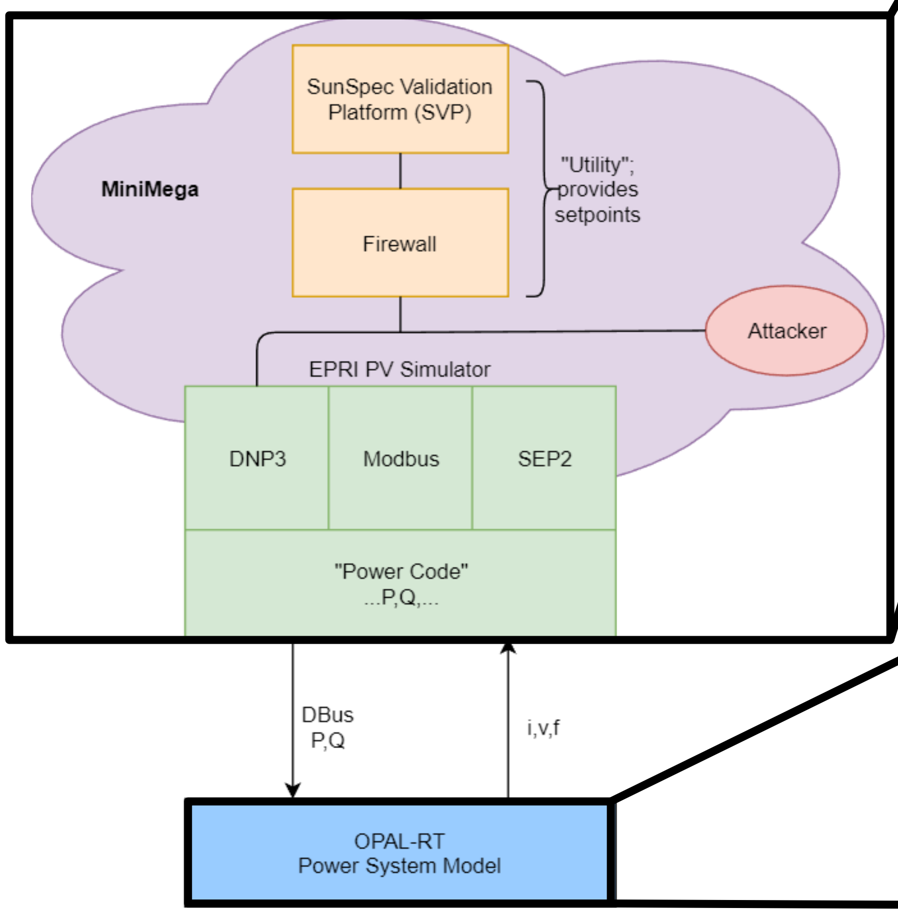
Simulate various attack scenarios to evaluate methodology

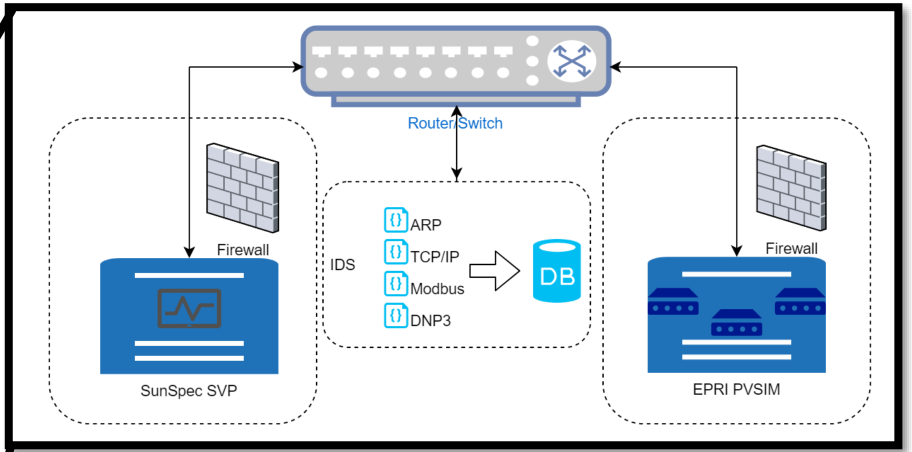


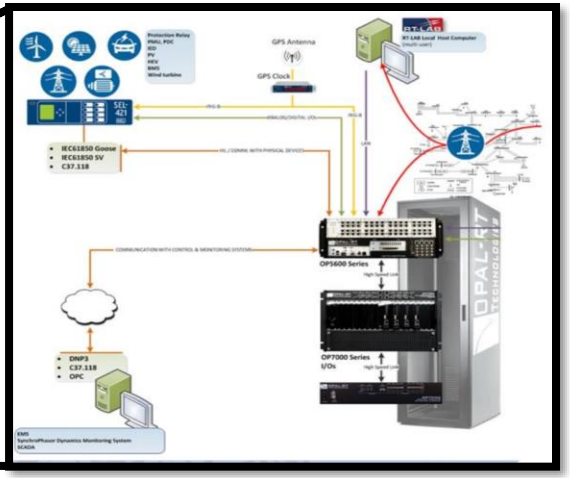
Emulation Environment

Create High-Fidelity Emulation Environment

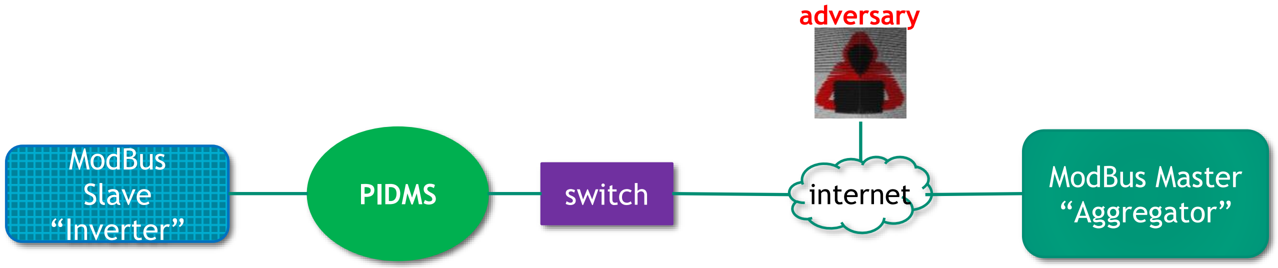
Constructing cyber-physical emulation environment that utilizes OPAL-RT software, EPRI's PV simulator, and Sandia's minimega tool.





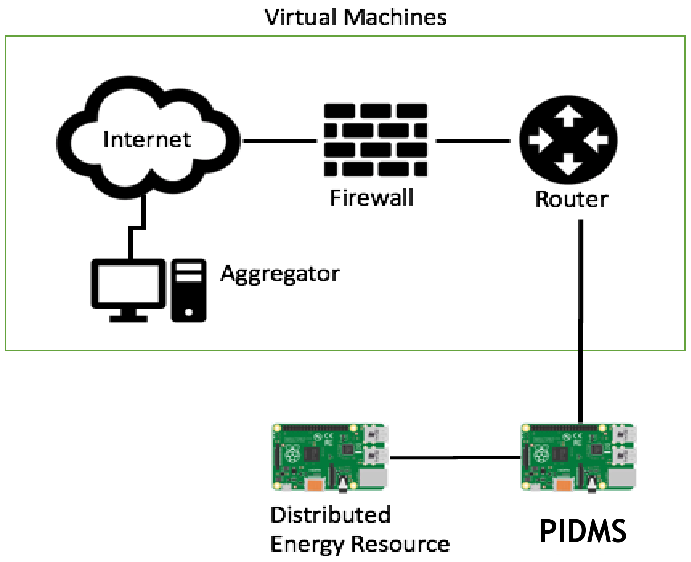


BITW Data Collection Sensor



The PIDMS sensor construction is underway

- Currently using a Raspberry Pi devices for the initial development
- Setup can emulate ModBus communications, a simple prototype of PIDMS, and adversary



BITW Data Collection Visualization

Hybrid IDS Approach

Cyber IDSs and Physical IDSs Individually are NOT Enough

Cyber detection

- Can detect suspicious behavior or known attack patterns
- Spoofed physical data may go undetected

Physical detection

- Fault detection models can detect malicious events that impact grid
- Cannot detect cyber attacks in early stages to thwart malicious events

Cyber-Physical detection is needed

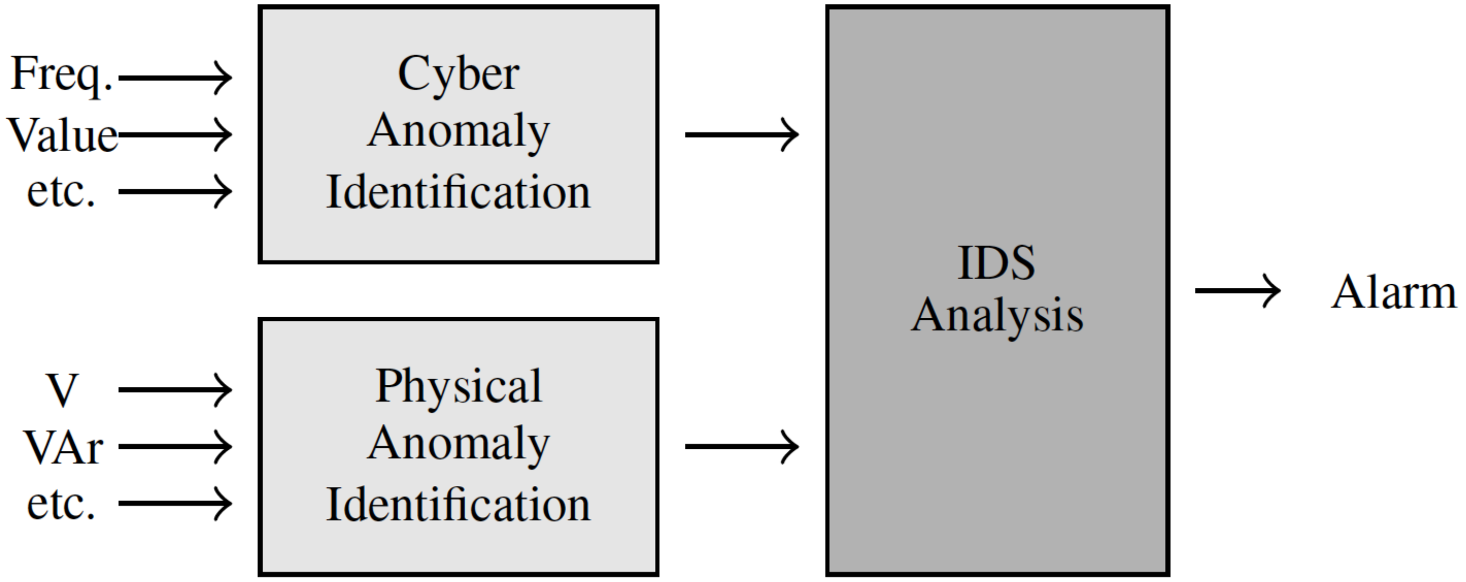
- Must monitor both cyber and physical data to perform effective detection in DER systems

Intrusion Detection/Prevention System Overview

Signature-Based	Match specific strings or sequence of bytes that are indicative of malware
	Can detect already existing malware that has already been observed
	Does not catch zero-day attacks or other attacks that do not have signatures
Behavioral-Based	Observe behavior and make classifications as normal or abnormal behavior
	Can potentially catch previously unseen malware
	Misclassification is possible, causing false-positives or false-negatives
Both approaches typically need access to full unencrypted data	Data can be network traffic, host events, host files, network/host resource utilization, etc.
Intrusion Prevention Systems automatically act/respond to detections	Block IP address, block packet, block executable, prevent future user logins, …

Hybrid Cyber-Physical IDS to Improve DER Security

- Must meet real-time constraints of DER (milliseconds or better)
- Increase difficulty of an adversary to defeat both a cyber-based and physical-based IDS that are correlating events
- Provide enhanced situational awareness for operators of a DER
- IDS requires higher throughput but can detect individual events



Hybrid IDS Features

- Combine signature and behavioral based IDS approaches
- Sensitivity analysis should be performed to determine relevant features on each system

Physical

- Voltage
- Current
- Active, apparent, & reactive power
- Frequency

Network

- Frequency
- Setpoint values
- Source/destination IP addresses
- Source/destination ports
- Sequence numbers
- TTL, checksum
- TCP flags
- Source/destination MAC addresses
- IP version
- Packet length
- Throughput
- Latency

Host

- File integrity
- Memory usage
- Processor usage
- Security logs

Demonstration: Need for Cyber-Physical IDS Features

False Data Injection – Through replay, man-in-the-middle, or other techniques, adversary alters setpoints sent to an aggregator

- Modbus or DNP3 without secure authentication

Insider Threat – Control setpoints altered by an insider

- Physical monitoring will be important

3 interoperable PV inverters (258 kW, 1 MW, and 10 MW)

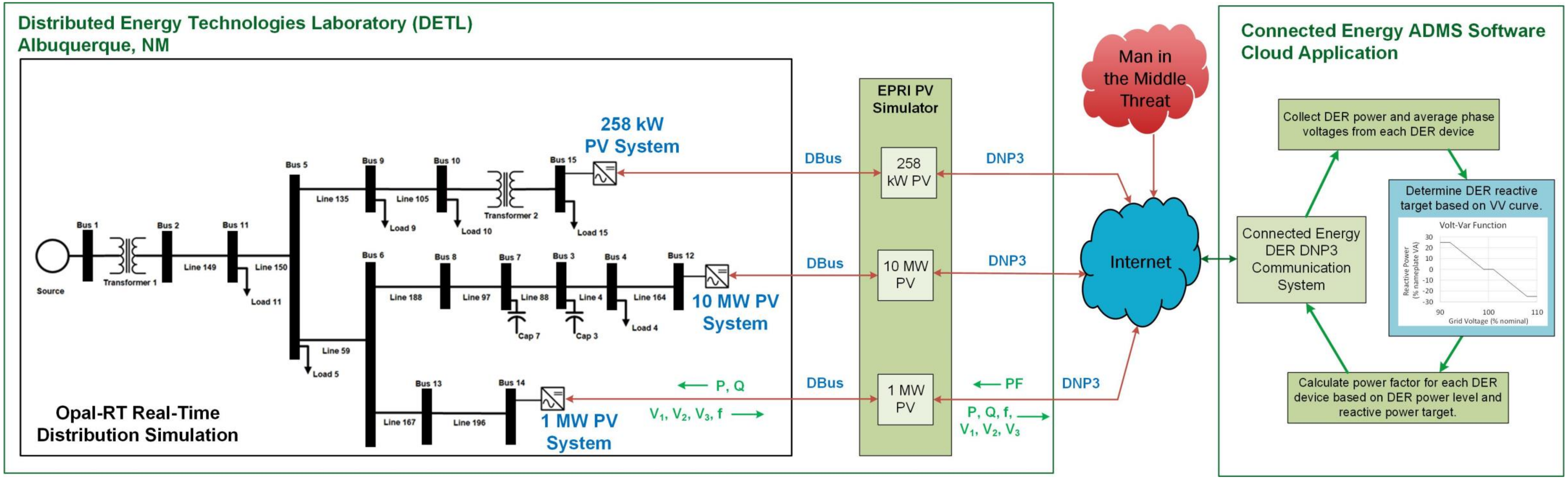
- 440% PV penetration
- Simulated using OPAL-RT 5600, 40 min simulation
- Modeled using EPRI DER Simulator
  - Hardware-in-the-Loop
  - DNP3 communications

Power measurements captured (AC power, reactive power, AC voltage, frequency, etc.)

Power Factor configurable

Experiment Setup

- Volt-VAr profile represented by points:
  - 92, 99, 101, and 108% of nominal voltage
- Reactive power profile represented by points:
  - 25, 0, 0, and -25% of the DER device
- Volt-VAr uses DETL reactive power capabilities to drive towards nominal voltage
- Adversary reversed sign of reactive power profile (-25, 0, 0, 25%)



Results

Good inverter case

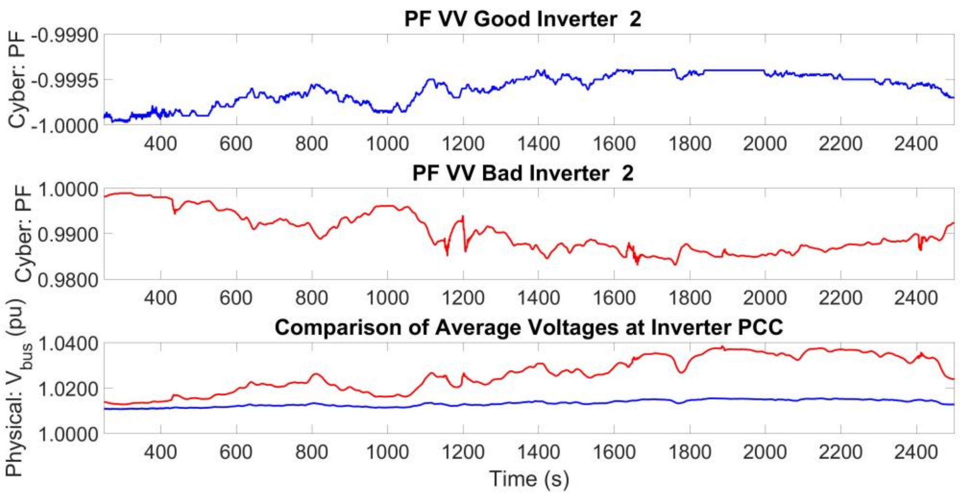
- Inverter absorbs reactive power
- Voltage at point of common coupling (PCC) close to nominal

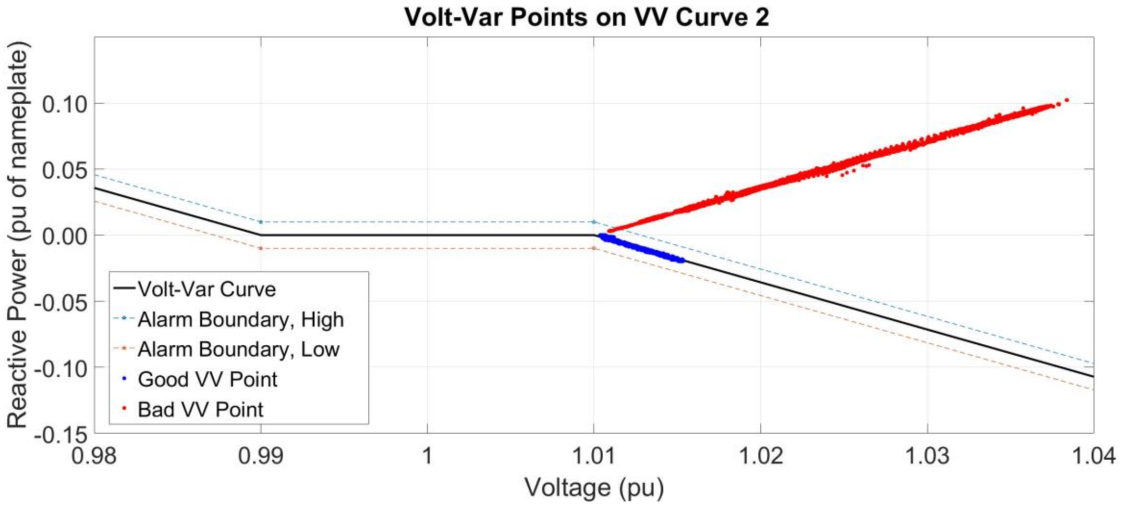
Bad inverter case

- Voltage increases significantly and diverges from nominal

Bounds were configured to alarm on Volt-VAr values

- In cases of no voltage or current measurement, physical data could be extracted





Results (Cont.)

The table below summarizes our tests with different data streams available

1. Cyber + Physical = Detects All
2. Cyber = Detects Cyber & Cyber-Physical
3. Physical = Detects Physical & Cyber-Physical
4. Partial Cyber + Partial Physical = Detects Physical & Detects Cyber-Physical
5. Partial Physical = Detects Physical & Cyber-Physical
6. Partial Cyber + Partial Physical = Only Detects Cyber-Physical
7. Partial Cyber + Partial Physical

	Physical Data				Cyber Data			
Case	Current Phasor	Voltage Phasor	Reactive Power	Detect	PF Write	V Read	Detect	Cyber & Physical Detect
1	✓	✓	✓	✓	✓	✓	✓	✓
2					✓	✓	✓	✓
3	✓	✓	✓	✓				✓
4	✓	✓		✓	✓			✓
5	✓	✓		✓				✓
6			✓			✓		✓
7		✓				✓		

Next Steps

- Further develop and implement Hybrid IDS approach on cyber-physical data collection sensor
- Test PIDMS as HIL in emulated environment
- Evaluate performance for different attack scenarios and iterate on IDS approach and data collection framework
- Develop response algorithms and evaluate in emulated environment

Thanks for listening!
Questions?

Shamina Hossain-McKenzie
shossai@sandia.gov

IDS Approaches Individually vs. Combined

Physical data monitoring

- Disconnect attack – Adversary controls large number of PV inverters and issues disconnect
  - Causes line overloads, frequency/voltage violation, system instabilities
- Volt-VAr attack – Adversary manipulates inverter control by injecting arbitrary levels of reactive power
  - Voltage magnitude and phase angle affected
- Excludes host and network based information

Cyber data monitoring

- Detecting malformed Modbus packets exceeding maximum length
  - Potentially leads to Denial of Service (DoS) attack
- Unauthenticated/cleartext protocols can be spoofed
  - Mis-information can cause an operator to believe normal operations or can provide unauthorized control
- Does not have the full picture of the physical data to validate observed data

Need to connect detected cyber events to physical events

- DOE GMLC "Threat Detection and Response" project distinguishes cyber events from physical events
- Cyber/Physical- detections help determine responses
- Other approaches focus on power system models to compare actual data against predicted data
  - Limited awareness of actual causes of failures/anomalies (can be hardware or software failures)