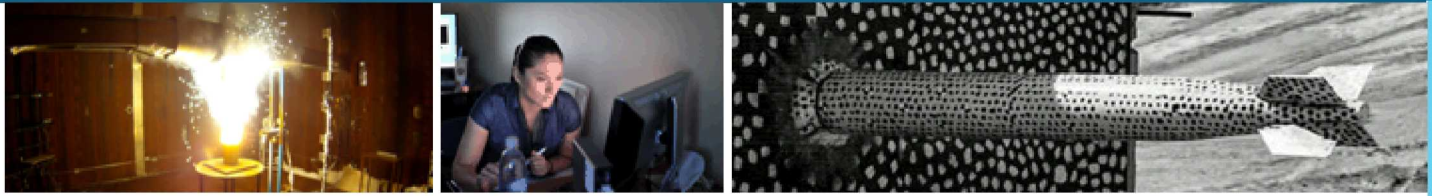
SAND2019-4795PE

Hybrid Intrusion Detection System Design for Distributed Energy Resource Systems



PRESENTED BY

Adrian R. Chavez
adrchav@sandia.gov

Team Members: Christine Lai, Nick Jacobs, Shamina Hossain-McKenzie (PI), Birk Jones, Jay Johnson, Adam Summers

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.

Isolated Cyber and Physical IDSs are Insufficient

High penetration of DERs

- Improved voltage regulation on distribution circuits
- Expanded distribution hosting capacity
- Wide-area damping
- Frequency control
- Ancillary service

Added power generation needs to be protected

- Aggregators subversion could impact power system reliability, stability, and safety

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

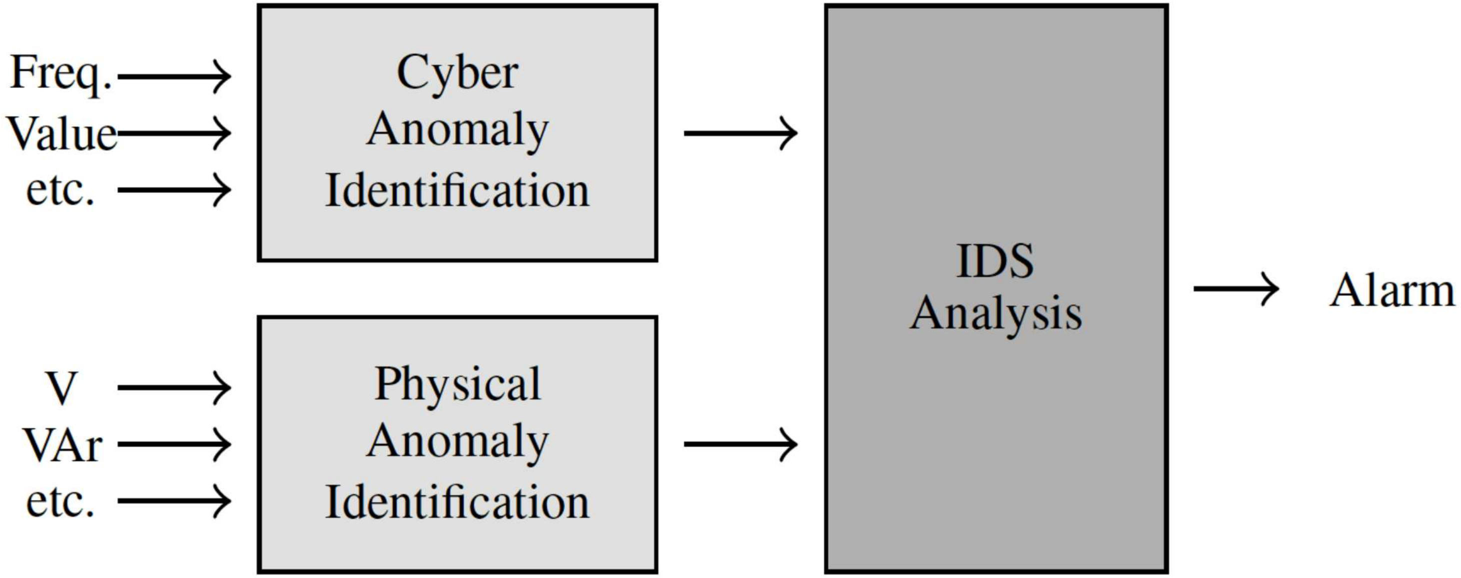
Cyber-Physical monitoring is needed

Intrusion Detection/Prevention System Categories

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, sensor measurements, etc.
Intrusion Prevention Systems automatically act/respond to detections	Block IP address, block packet, block executable, prevent future user logins, etc.

Hybrid Cyber-Physical IDS to Improve DER Security

- Requires higher data throughput to meet real-time constraints of DER (milliseconds or better)
- Event correlation matches multiple data streams to a single event
- Provides enhanced situational awareness for operators of a DER
- Increases difficulty for an adversary to defeat both a cyber-based and physical-based detection



Hybrid IDS Features

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

Combine signature and behavioral based IDS approaches

Sensitivity analysis should be performed to determine features on each system

Experiment Scenarios

False Data Injection (control settings) – Replay, man-in-the-middle, or other techniques to alter setpoints sent to an aggregator

- Modbus or DNP3 without secure authentication

Insider Threat – Physical features may be intercepted and altered by an insider

- Physical monitoring will be important

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

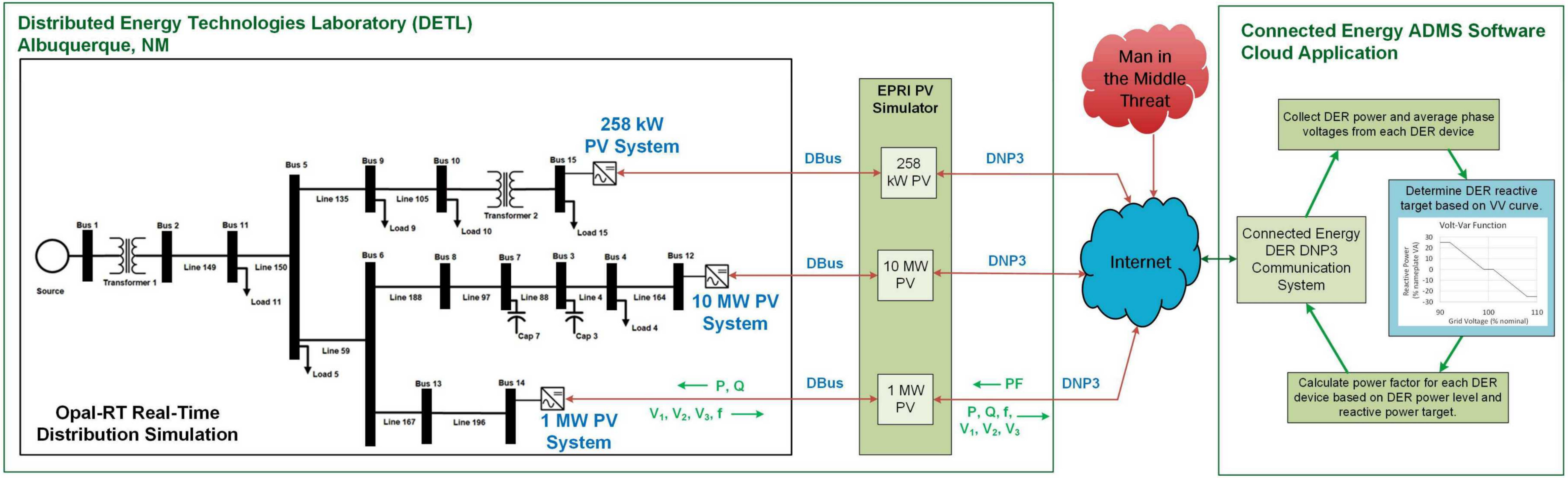
- 440% PV penetration
- Simulated using Opal-RT 5600
- Modeled using EPRI PV simulator
  - Hardware-in-the-Loop
  - DNP3 communications

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
- Insider threat reversed sign of reactive power profile (-25, 0, 0, 25%) (MITM also applies)



Distributed Energy Technologies Laboratory (DETL)
Albuquerque, NM

Opal-RT Real-Time Distribution Simulation

Connected Energy ADMS Software Cloud Application

Collect DER power and average phase voltages from each DER device

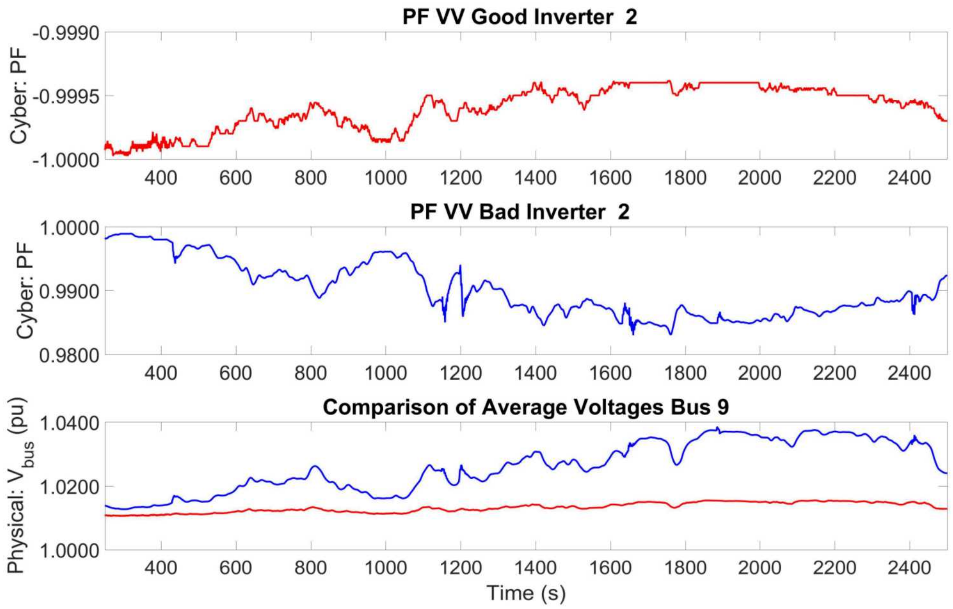
Determine DER reactive target based on VV curve.

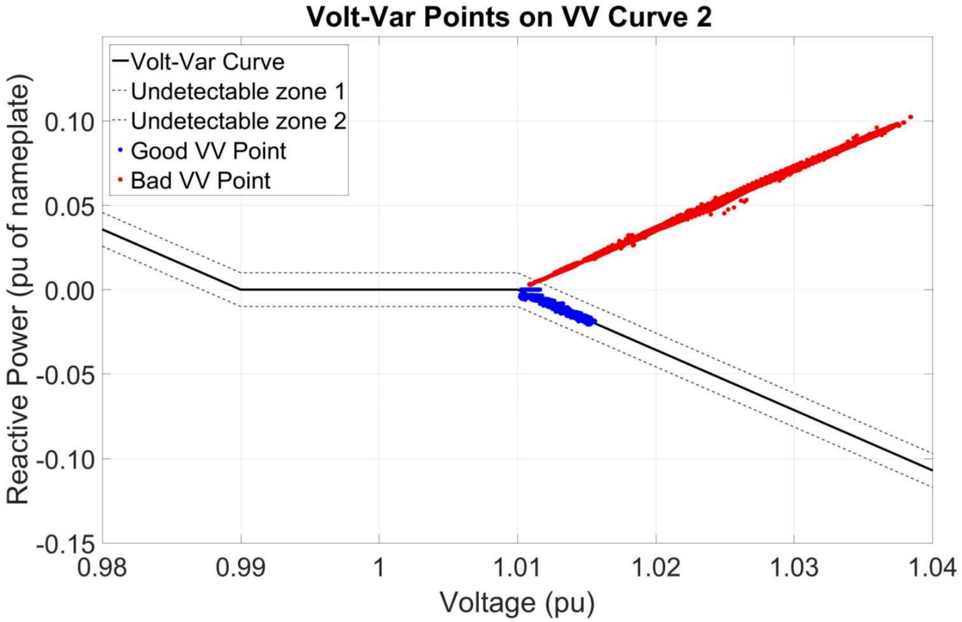
Calculate power factor for each DER device based on DER power level and reactive power target.

Connected Energy DER DNP3 Communication System

Results

- 40-minute simulation
- Inverter absorbs reactive power in good inverter – voltage at Point of Common Coupling (PCC) close to nominal
- Bad inverter, voltage increases significantly
- Bounds were configured to alarm on Volt-VAr values – In cases of no voltage or current measurement, physical data could be extracted

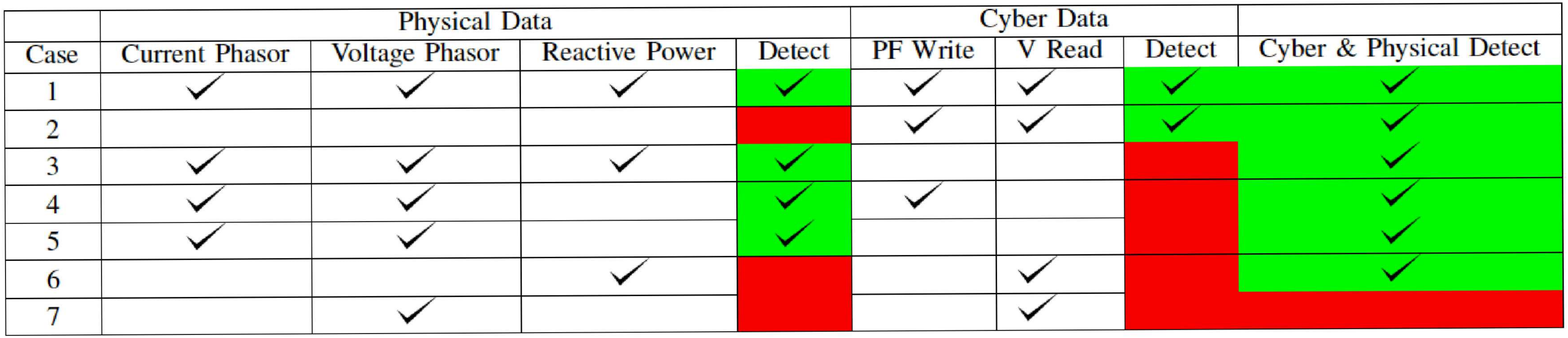




Results (Cont.)

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 = None Detected



	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		✓		🟥		✓	🟥	🟥

Individual vs. Combined IDS Data Monitoring Approach

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)

Questions

Adrian R. Chavez
adrchav@sandia.gov

Shamina Hossain-McKenzie
shossai@sandia.gov