U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Cybersecure Interconnection of Distributed Energy Resources

Lawrence Livermore National Laboratory (LLNL)

Emma Stewart (PM), Jhi-Young Joo (PI), Benjamin Salazar, Nan Duan, Nathan Yee

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Cyber adversaries have a significant range of capabilities and interests

Tier	Adversary	Definition
6	Top Tier Nation-State	**Full spectrum operations**: Combine cyber capabilities with significant military and intelligence capabilities to achieve specific outcomes
5	Sophisticated State Actor	**Create vulnerabilities** by impacting product design or supply chain to enable exploitation of systems of interest
4	Organized Criminal Organization or State Actor	Discover **unknown vulnerabilities** and develop exploits, working in highly proficient and **well-funded teams**
3	Sophisticated Individuals and Small Groups	Discover **unknown vulnerabilitie**s and exploit using sophisticated tools and techniques
2	Individual Hacker	**Develop new tools** to exploit publicly **known vulnerabilities**
1	Script Kiddie	**Utilize tools** and strategies developed by others to exploit publicly **known vulnerabilities**

Strategy for a secure and resilient electric grid

	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify	Risk Assessment, Asset Inventory and Management, Critical Failure/Component Analysis		
Protect	Basic cyber hygiene	Encryption, Network Segmentation, Cyber grid planning tools	Firmware verification, Control verification
Detect	Anti virus	Data aggregation, threat detection (MMATR)	Cross-domain operational intelligence, novel data analytics for threat detection
Respond	Manual mitigation of known threats	Orchestration and remediation	Cyber-physical fault isolation, dynamic network segmentation
Recover		OT forensics analysis tools, cyber event reconstruction	Optimized black start strategies leveraging DER
Endure	Microgrids, Component diversification, Cyber safe mode		

Strategy for a secure and resilient electric grid

	Adversary Tier 1&2	Adversary Tier 3&4	Adversary Tier 5&6
Identify	**Cybersecure Interconnection of DER**		
Protect	Basic cyber hygiene	Encryption, Network Segmentation, Cyber grid planning tools	Firmware verification, Control verification
Detect	Anti virus	Data aggregation, threat detection (MMATR)	Cross-domain operational intelligence, novel data analytics for threat detection
Respond	Manual mitigation of known threats	Orchestration and remediation	Cyber-physical fault isolation, dynamic network segmentation
Recover		OT forensics analysis tools, cyber event reconstruction	Optimized black start strategies leveraging DER
Endure	Microgrids, Component diversification, Cyber safe mode		

Summary: Cybersecure Interconnection of Distributed Energy Resources (DER)

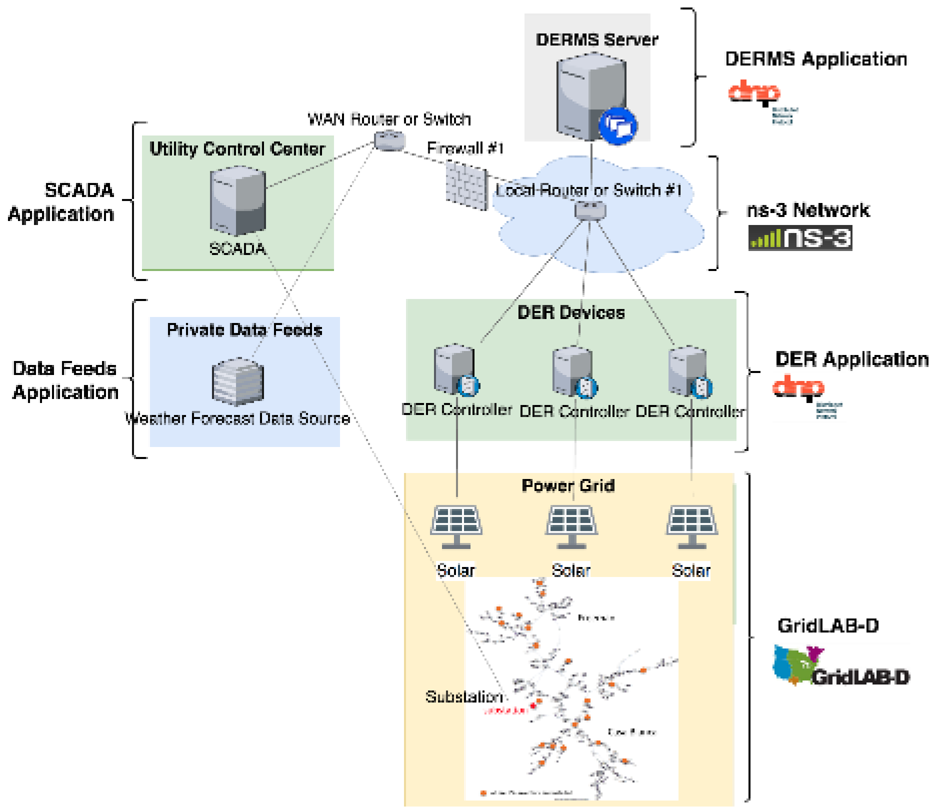
Objective

- Develop a tool that can evaluate the cybersecurity risk of various DER integration architectures, and design remediation strategies for a grid with high-penetration of DER can become more resilient and better able to survive a cyberattack

Schedule

- October 2017 – September 2019
- Key deliverables
  : Report on attack strategies and 10 cybersecurity scenarios (Oct 2018); models and methods for remediation and prevention of attack consequences (Mar 2019); 2 conference papers on framework and scenarios (Oct 2019)
- Expected capability
  : streamlined analyses for utilities and product vendors to use best practices for cybersecurity protection during DER interconnection, without increasing cost or time

DER Control and Communication Architecture



Total Value of Award:	**$ 2.5M** (no cost share)
Funds Expended to Date:	**50.9%**
Performer:	**LLNL**
Partners:	**SGS, RevSec, HECO, RPU, SolarEdge, Eaton, PSL**

Advancing the State of the Art (SOA)

Current "state of the art"

- **Interconnection tools and scenario analysis** developed through numerous EERE funded projects
- Numerous publications on the **impact of high penetration of PV** on the distribution and bulk systems
- **Cybersecurity plans** often specific to interconnecting technology → no analysis on wide-scale impact and multiple threat areas with a significant number of controllable inverters

Our approach

- Leverage co-simulation work at LLNL to develop a tool to give **a broad picture of impact of cyber security in the DER space**
  → prioritization of remediation strategy based on impact and attack vector analysis
- **Utility and vendor interaction** for sanity checks and rapid transition of research results
  → no increase in time and cost for cybersecurity analysis of DERs
- Coupling of **power grid and cyber expertise** for a full range of potential scenarios and solutions
  → leverage LLNL's core capabilities in power system and cybersecurity research

Challenges to Success

Challenge 1: data acquisition

- NDAs and IP Management Plan with project partners
- Multiple sources for grid models and data

Challenge 2: co-simulation and integration of tools

- Leverage existing platform from GMLC projects

Challenge 3: relevance to current industry needs

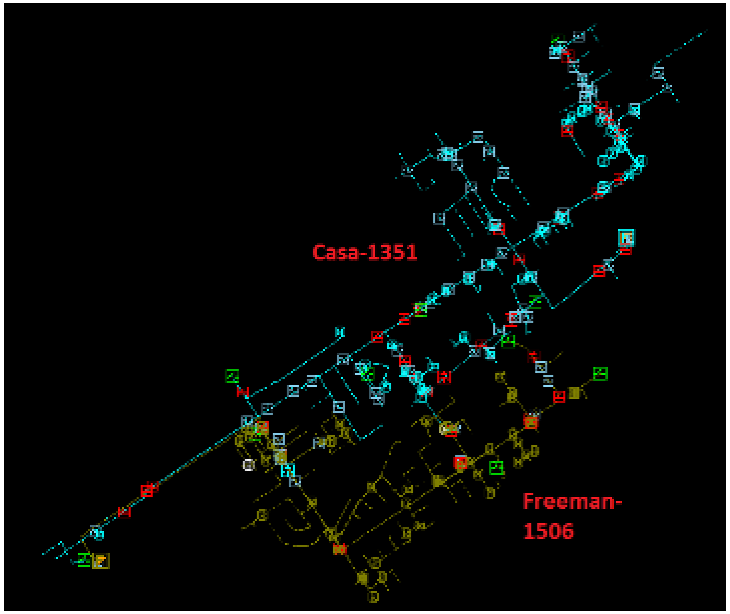
- Working group meetings for industry feedback
- Regular meetings with project partners
- Major deliverables reviewed by industry including project partners

Progress to Date: Grid Model Validation

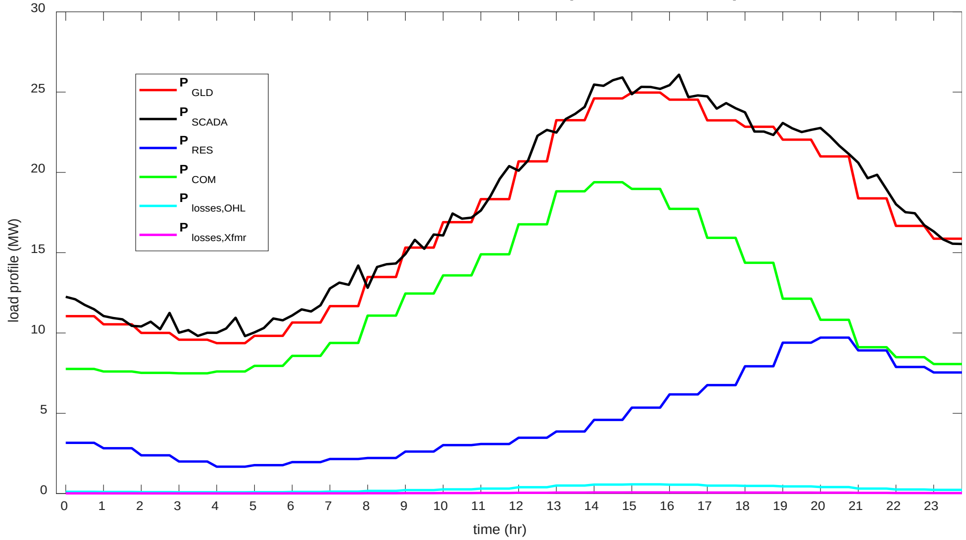
Major Accomplishments

- **Milestone 1**: Accuracy of distribution and communication model is verified to be >90% reviewed against existing measured data from the utility on a test feeder.
  → achieved accuracy over 96%

$$\text{accuracy} = 1 - \frac{\sqrt{\frac{\sum_{k=1}^{N}\left(P_{SCADA,k} - P_{GLD,k}\right)^2}{N}}}{\max\left(\left(P_{SCADA,peak}, P_{GLD,peak}\right)\right)}$$



Casa Blanca and Freeman feeder models of Riverside Public Utilities



SCADA data and GridLAB-D simulation results of a Riverside Public Utilities model

Progress to Date: Cybersecurity Scenarios

Major Accomplishments

- **Milestone 2**: 10 scenarios (combined or singular events) selected, being reviewed by technical advisory group for accuracy and likeliness

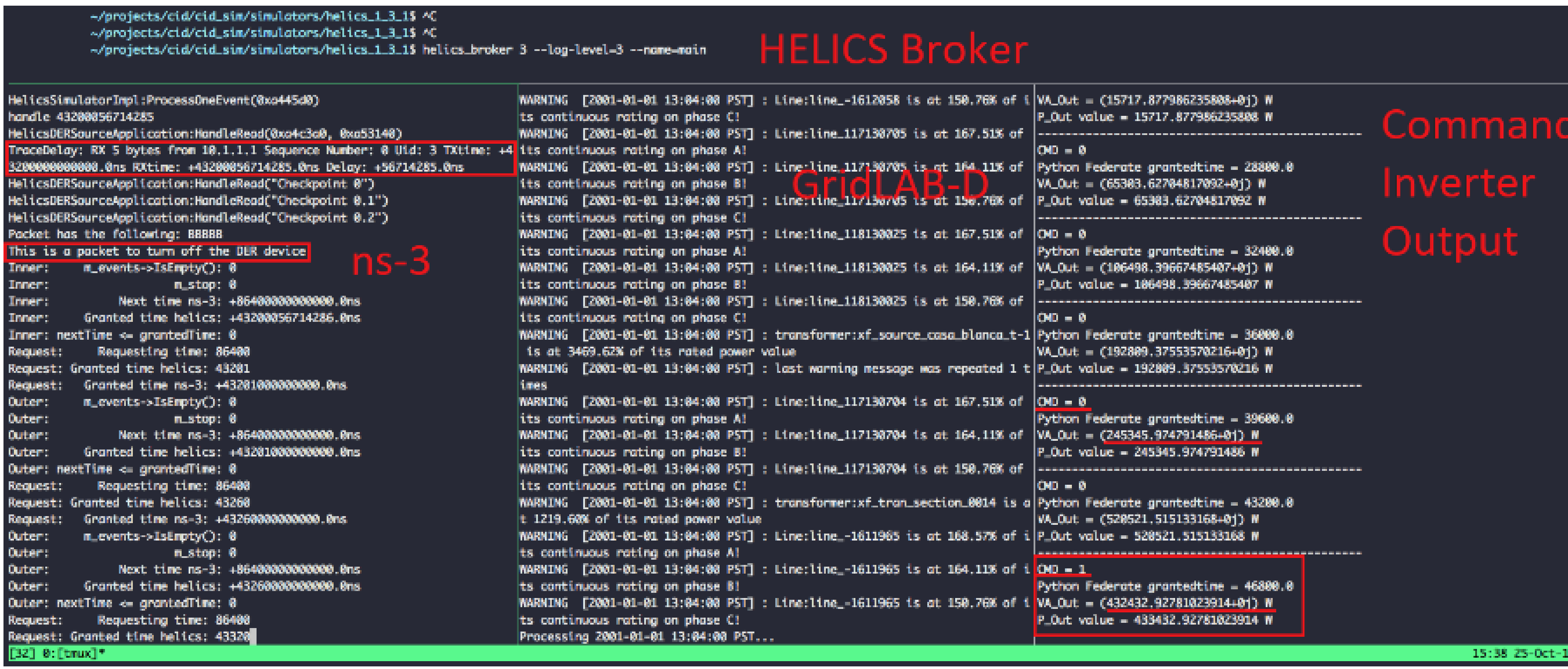
Impact (from low to high) **Cyberattack Vector**	**Incorrect dispatch of DER** (unnecessary usage, financial loss)	**Instability at customer sites** (DER/generation/loads)	**Distribution impacts** (transformer overload via sudden increase in loads)	**Transmission impacts** (under/over-frequency load shedding to large scale outage)	**Safety hazard** (anti-islanding by unintended desynch or resynch)
Configuration/operational setting Change		7	9	1, 3, 5	9
Firmware/software Change		6, 7	9	2, 4, 5	
Compromised communications	10	7		10	8
Timing attack			9	10	8
Improper verification of messages	10		9		
Data feed change	10			10	
Time scale	Steady state (DERMS dispatch interval; 5-60 minutes)	Dynamic (seconds)	Steady state (SCADA interval; ~15 minutes)	Dynamic/steady state (seconds to minutes)	Dynamic/steady state (seconds to minutes)

Severity of impact →

Progress to Date: Co-Simulation of Grid/Comm

Major Accomplishments

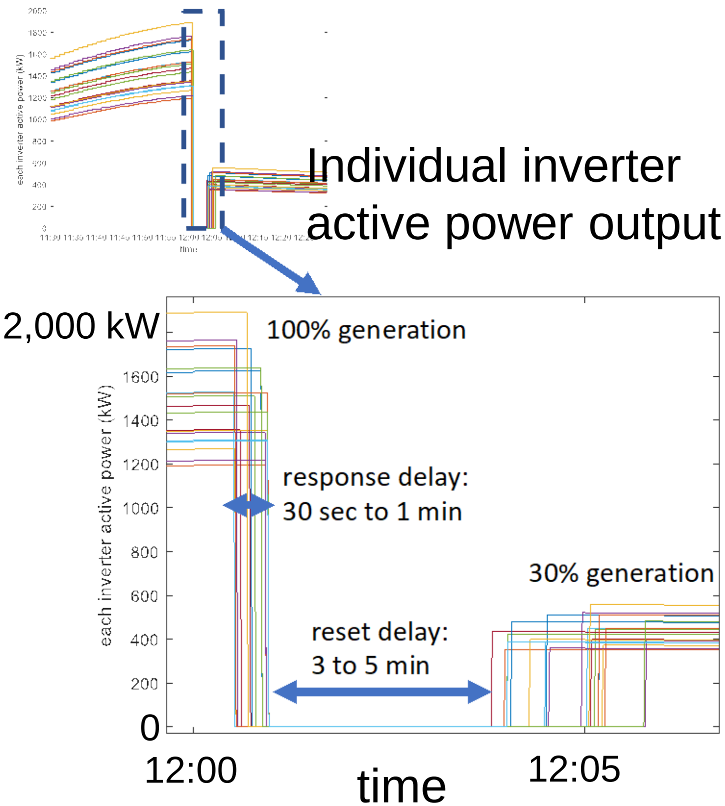
- Co-simulation functionality
  → coupling of ns-3, GridLAB-D feeder model, and inverter module

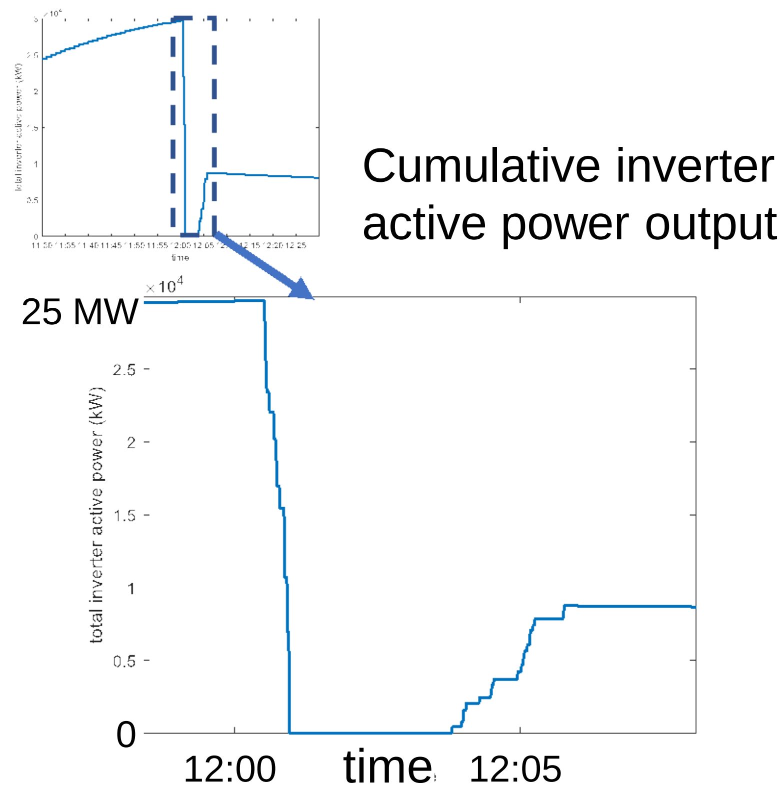


Progress to Date: Simulation of Physical Impacts

Preliminary scenario simulation results

- Cyberattack model → impact on a physical model
- At solar generation peak, malicious command issued to trip off all inverters and bring them back to 30%

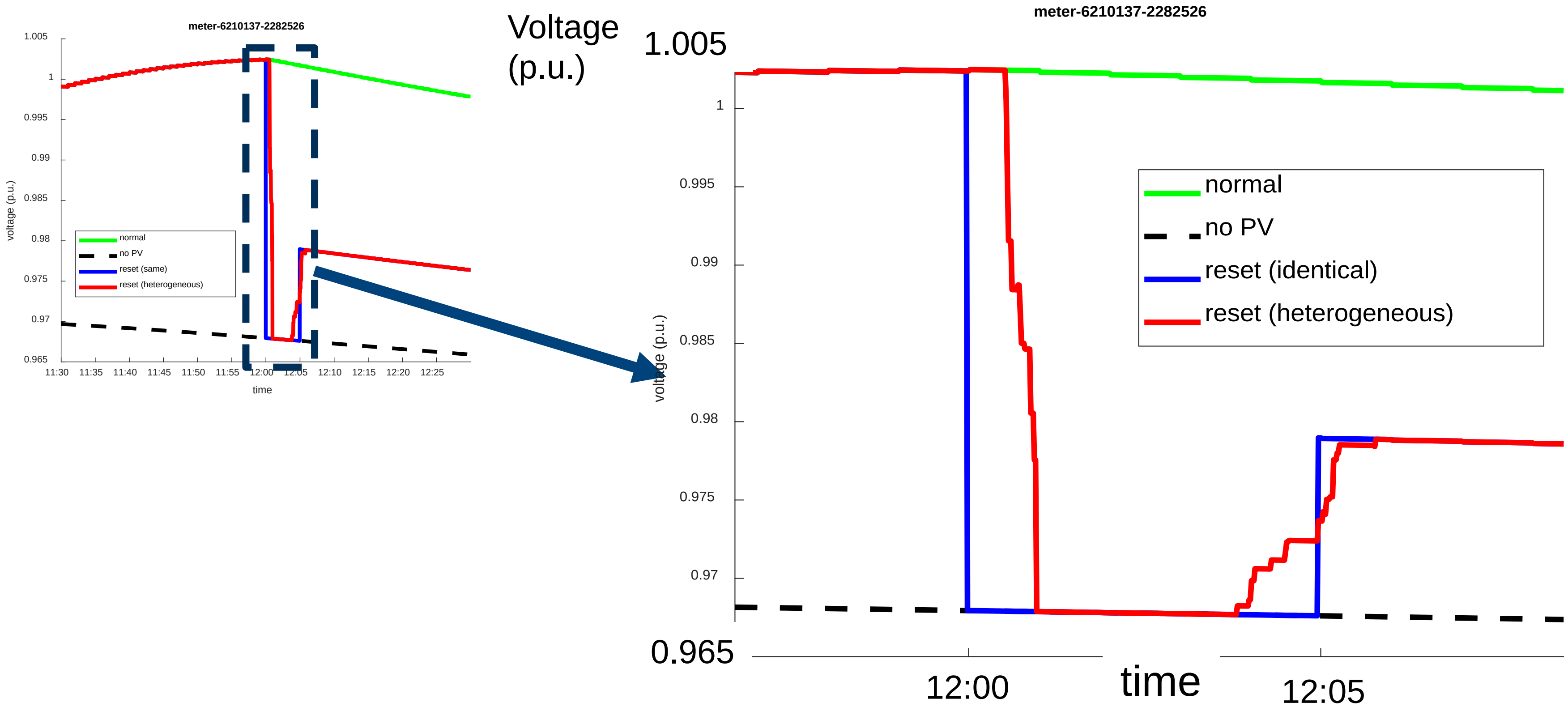




Progress to Date: Simulation of Physical Impacts

DER controller modeling accuracy

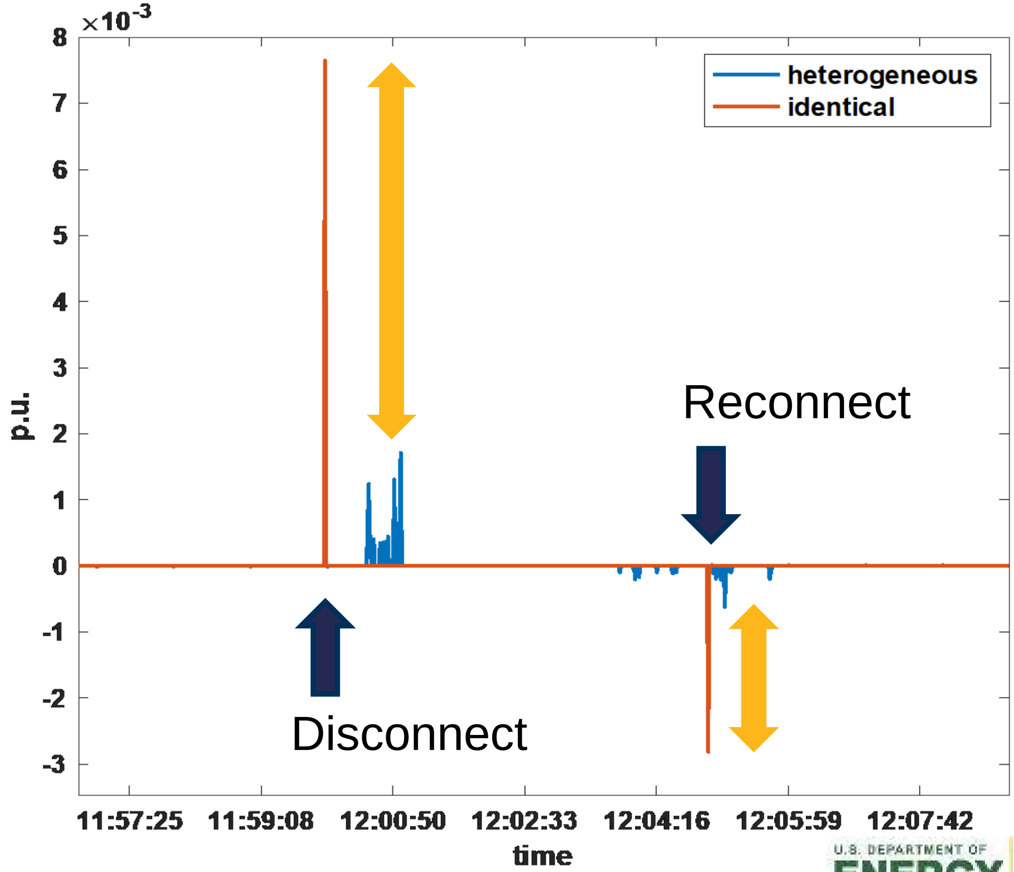
- But if all inverters had the same communication and control settings…



Progress to Date: Simulation of Physical Impacts

DER controller modeling accuracy

- Voltage stability comparison (at substation level)
  : Voltage differences between two consecutive time steps



Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- **Targeted end users**
  : utilities, power system planning tool vendors, DERMS vendors
- **Plans for industry acceptance**
  - Project partnership includes targeted end users
  - Solicitation of industry feedback through utility working group meetings/workshops
  - Commercialization effort based on IP Management Plan among partners

Next Steps for this Project

Approach to the end of project

- **Milestone 4**: **Mitigation strategy scenarios** are designed for simulation and for each attack scenario from Phase 1. Range of required capabilities is available in simulation tool (Mar 2019)
- **Milestone 5**: **Remediation and evaluation strategies** for each attack are presented in a report to utility staff and working groups. Pathways for response are established. If no pathway can be found it will be presented as a high risk scenario and research on new protection methods evaluated. (May 2019)
- **Milestone 6**: **Prototype** utilized to simulate a second region with utility partner and results approved with working group team (Sep 2019)
- **Milestone 7**: Presentation at **utility working group meeting**, and 2 **conference papers** published on framework and scenarios (Oct 2019)

Thank you