U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Cybersecurity via Inverter Grid Automatic Reconfiguration (CIGAR)

Lawrence Berkeley Lab

Daniel Arnold and Sean Peisert

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

Project Overview

Objective

- CIGAR uses Reinforcement Learning (RL) to control non-compromised solar inverters to mitigate destabilizing effects of inverters that have been compromised as part of a cyber attack.

Schedule

- April 1, 2018 – Mar. 31, 2021
- Task 1 – Feedback control modeling (completed Mar. 31, 2019).
- Task 2 – RL algorithm and prototype software development (completed Mar. 31, 2020).
- Task 3 – Integration of RL agent into NRECA Open Modeling Framework (in progress, due Mar. 31, 2021).

Total Value of Award:	**$ 2,500,000**
Funds Expended to Date:	**% 66%**
Performer:	**Lawrence Berkeley Lab**
Partners:	**Siemens CT, Ariz. State University, NRECA**

Advancing the State of the Art (SOA)

- (SOA) Current SOA for defending the grid against cyberattacks looks at behavior of individual systems (e.g. DER, voltage regulation systems).
  - *Stability issues arising from complex interaction between these systems has not been addressed.*
- (Feasibility) CIGAR uses reinforcement learning to understand the holistic behavior of the entire system, in the context of cyber attacks against a subset of inverters and adjust settings of remaining inverters to maintain grid stability.
  - *Reinforcement Learning has demonstrated the ability to find optimal control policies in systems with complex dynamical interactions via intelligent simulation (i.e. "smart" trial and error).*
- (Pushing SOA) Optimization of dynamic systems with mixed states is extremely challenging. The tools developed for CIGAR are able to find controllers that take into account other dynamics in the system (e.g. regulator action).

Advancing the State of the Art (SOA)

- (Benefit to End User) CIGAR provides the means to learn control policies 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.
- (Advance CEDS) 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.
- (Adoption Potential) Task 3 of CIGAR focuses on integration of the reinforcement learning agent into the NRECA Open Modeling Framework, allowing utilities to upload system models for agent training and simulation.
    - Analysis could lead to system hardening on network specific basis.

Progress to Date

Major Accomplishments

- Reinforcement Learning algorithm and software prototype complete (Mar. 31, 2020).
  - Proximal Policy Optimization (PPO) used for continuous and discrete action spaces.
- Alpha version of API for Open Modeling Framework complete (Mar. 31, 2020).
- Paper accepted to SmartGridComm 2020: "Deep Reinforcement Learning for DER Cyber-Attack Mitigation".
  - Focuses on the use of RL to adjust settings in DER to mitigate voltage oscillation attacks.
- Paper accepted to SmartGridComm 2020: "SoDa: An Irradiance-Based Synthetic Solar DataGeneration Tool".
  - Highlights a synthetic solar generation tool to create realistic sub-minute solar photo-voltaic (PV) output power time series.
- Paper submitted to 2020 American Control Conference: "Deep Reinforcement Learning for Mitigating Cyber-Physical DER Voltage Unbalance Attacks".
  - Focuses on the use of RL to adjust settings in DER to mitigate large voltage imbalances due to cyber attacks.

Challenges to Success

Challenge 1 – No Reinforcement Learning/Grid Simulation Tool

- At the beginning of this project, there was no available software tool that integrates reinforcement learning capabilities with distribution grid simulations.
- Mitigation: The project team integrated popular and stable software (RLLib/Ray with OpenDSS) creating a software framework for RL applied to distribution grids.

Challenge 2 – RL Agents Often Difficult To Train

- Very young field, evolving quickly, many approaches (algorithms). Often unclear why one approach will work and another will not. Very sensitive to hyperparameters!
- Mitigation: The project team developed adaptive control approaches to mitigate DER-driven instabilities. These served as a baseline for comparison in RL agent training.

Challenge 3 – Encouraging Utility Adoption

- Algorithms are very complicated. We want to streamline utility interaction and not create impediments for adoption.
- Mitigation: Mask details of RL agent training from users. Ensure RL agents adjust DER settings in IEEE 1547 compliant manner.

Collaboration/Sector Adoption

Plans to transfer technology/knowledge to end user

- CIGAR is beneficial for energy companies, vendors, researchers.
  - Utilities can simulate cyber attacks on DER on their networks and use RL agents to test defensive strategies. This could lead to system hardening decisions (e.g. choosing "cyber-resilient" default values for smart inverter functions).
  - DER vendors can integrate the defensive agent neural networks onto their devices to allow non-compromised units to directly participate in cyber-attack mitigation.
  - Researchers can use the CIGAR framework to optimize distribution grids with nonlinear dynamics for a variety of other objectives and/or using other controllable devices (such as EVs).
- Path to Industry Acceptance: Integration of RL agent training and simulation capabilities directly into the OMF.
  - Allows co-ops and other utilities to interact with CIGAR technology in a familiar tool.
- Project team will be running experiments over the remaining months of the project testing the RL agent performance in variety of scenarios (grid size, solar conditions).
- Project team will hold an end of project workshop to demonstrate technology to co-ops.

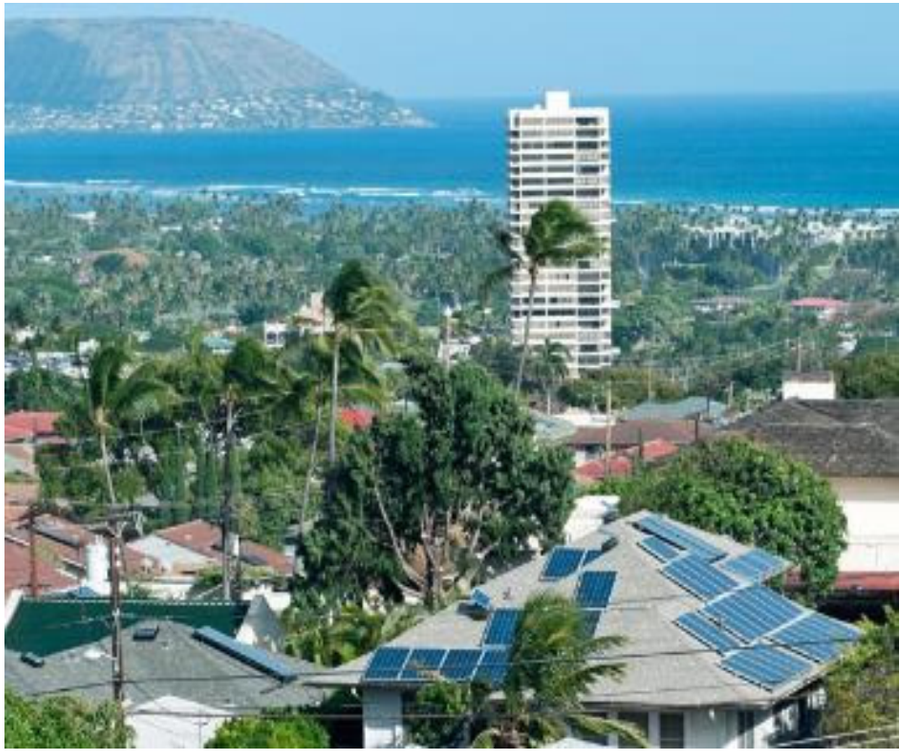
Next Steps for this Project

Approach until end of project (Mar. 31, 2021)

- Key Milestones
  - Training of Reinforcement Learning Controller on unbalanced network with 1000+ buses.
  - Validate RL agent behavior in different seasonality and solar conditions.
  - Complete Task 3 – Integration of RL defensive agent software into Open Modeling Framework.
  - Journal publication highlighting RL agent performance across different grid topologies and external conditions (peak conditions, season, etc.) interacting with protection and voltage regulation systems.
  - (Time permitting) investigate methods to decentralize agent deployment.
    - Agents are centrally trained, but for some objectives (voltage balancing) the agent requires information shared from nearby DER. The project team is investigating ways to extend RL agent training to infer nearby grid conditions from purely local measurements.
- Upcoming significant events
  - CIGAR Year 3 workshop to demonstrate OMF CIGAR API for NRECA co-ops (March 2021).

Additional Slides - Motivation

Problem: Standardization of DER Smart Inverter Controls



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

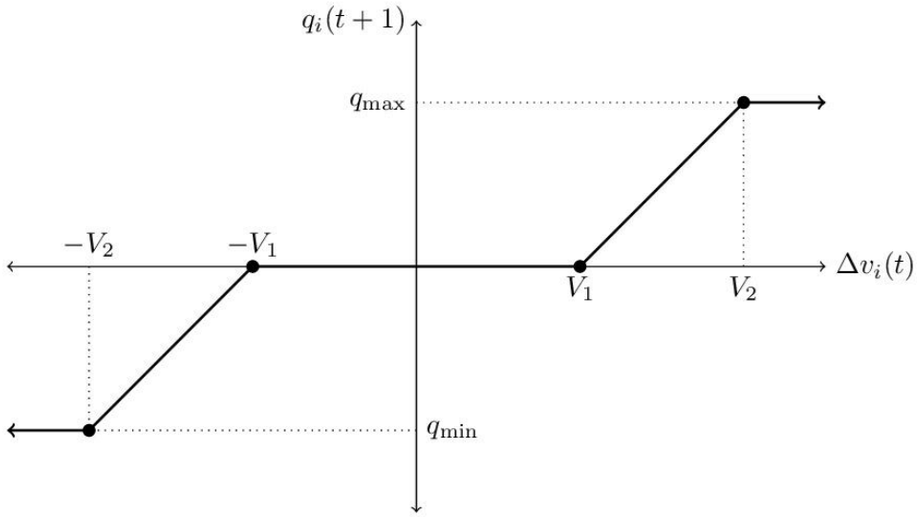
"…Enphase used built-in communications links to upgrade the grid-stabilizing capacity of four-fifths of Hawaii's rooftop solar systems"

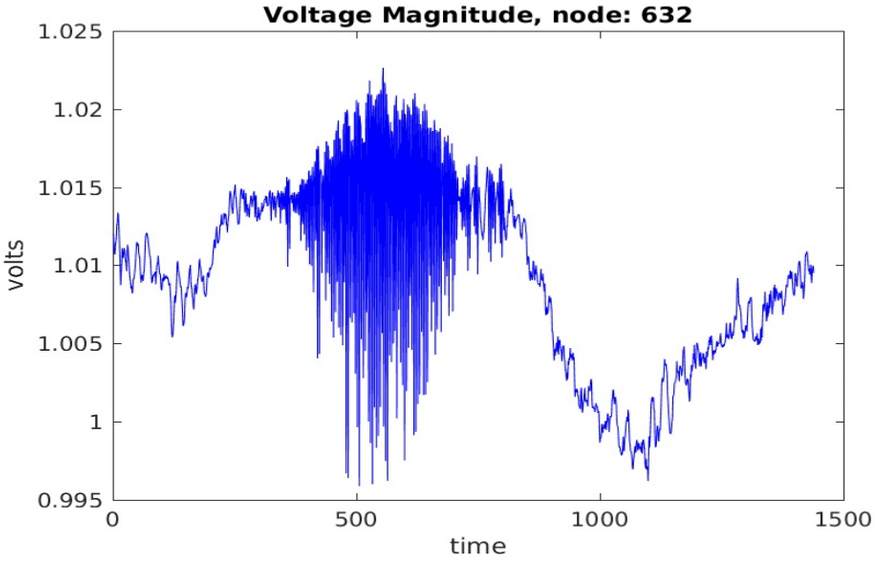
https://spectrum.ieee.org/energywise/green-tech/solar/in-one-day-800000-microinverters-remotely-retrofitted-on-oahu

If compromised, what would happen?
How can we defend against this?

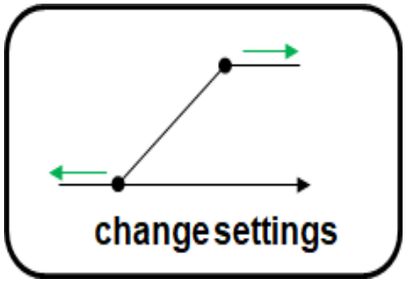
Additional Slides – Problem Definition

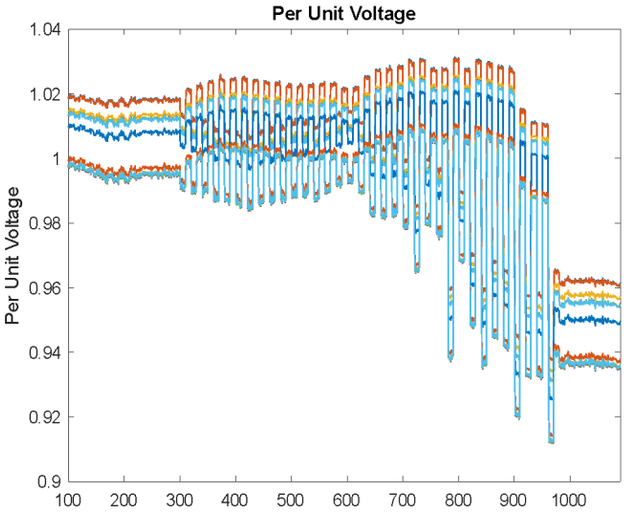
Cyberattack on DER Smart Inverter Settings





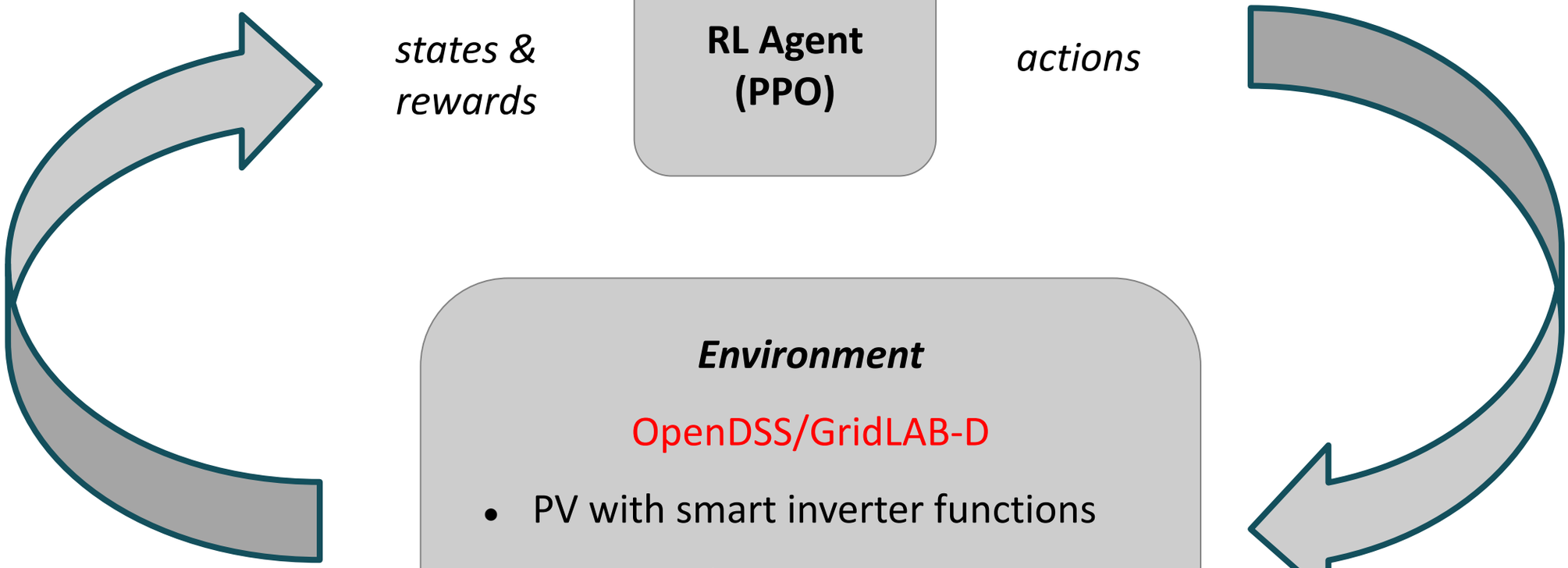
CIGAR adjusts DER settings in *non-compromised* units





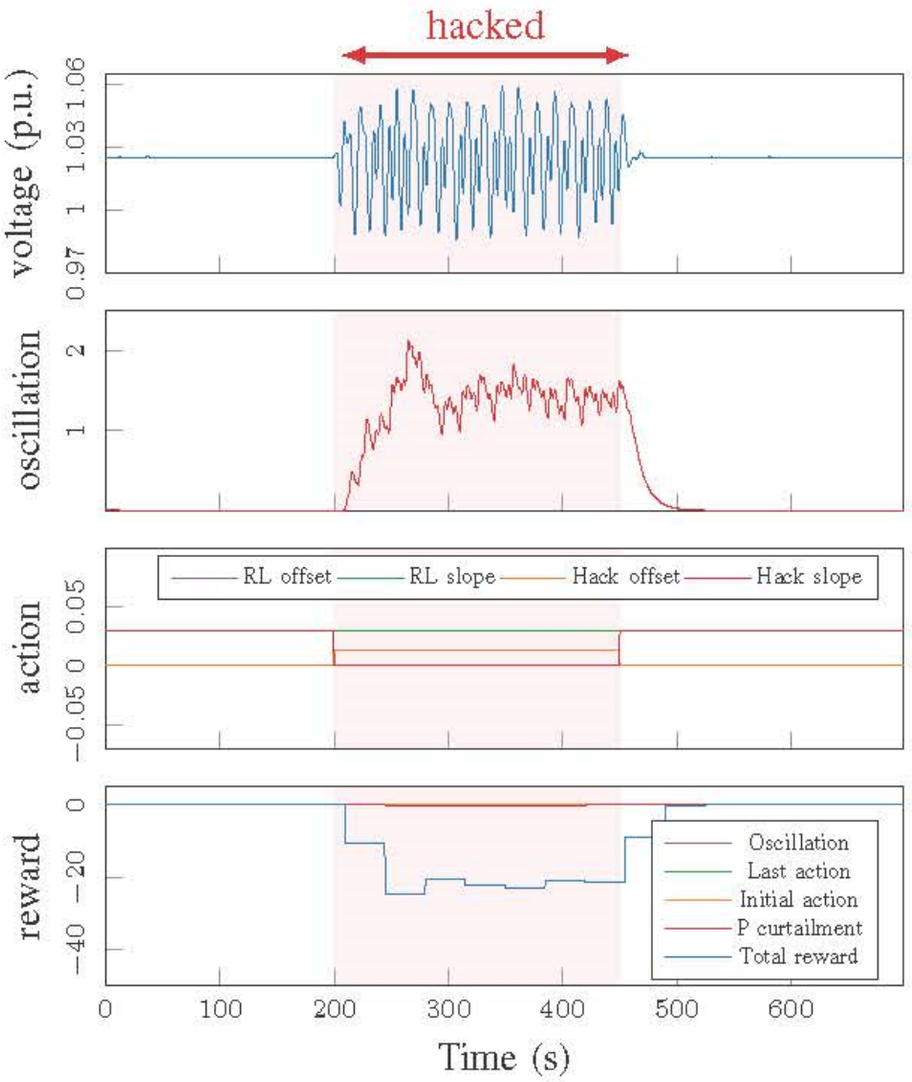
U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Additional Slides – Reinf. Learning

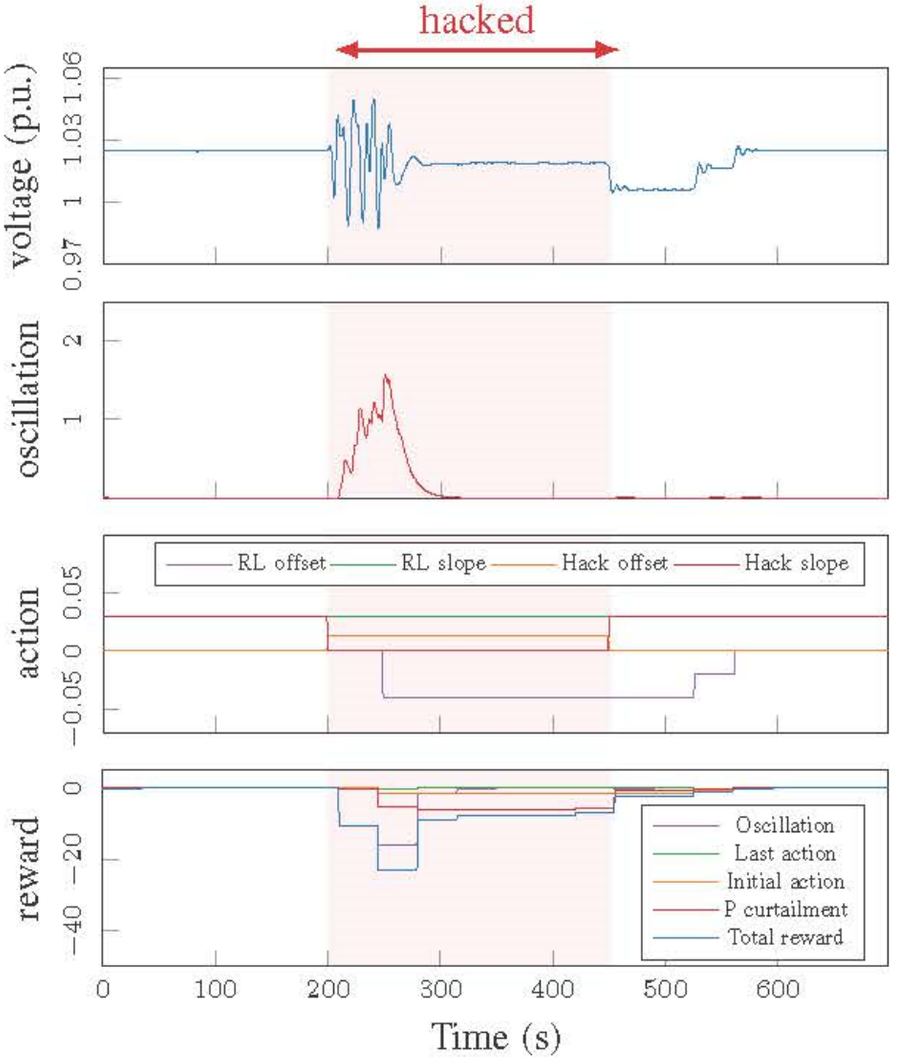


Additional Slides - Results

No Control

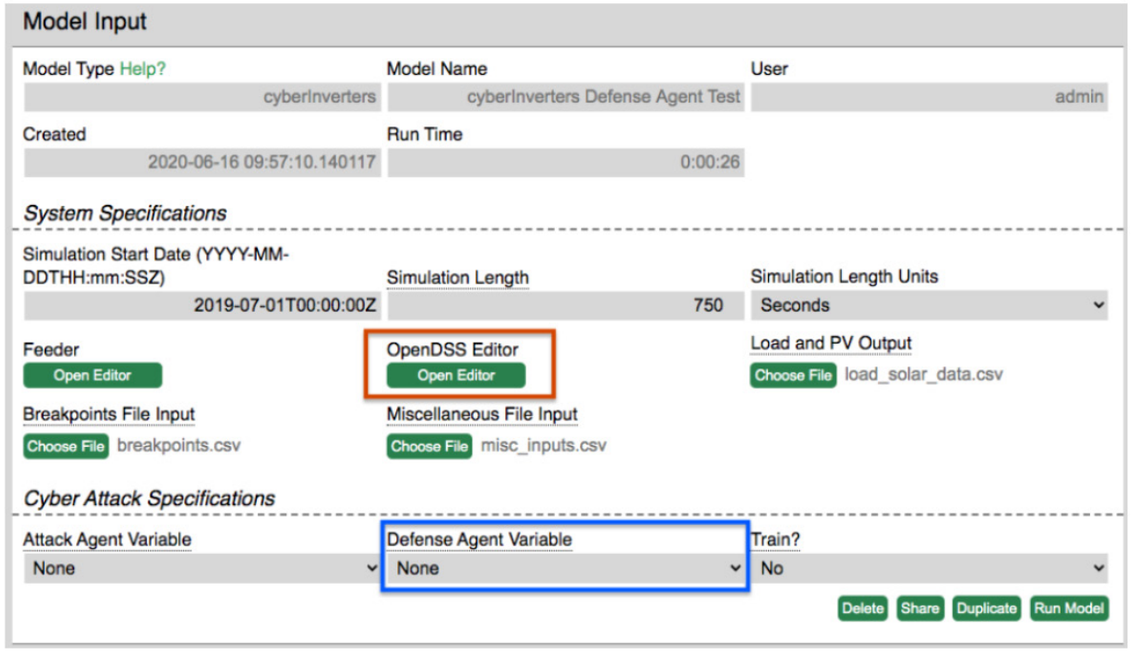


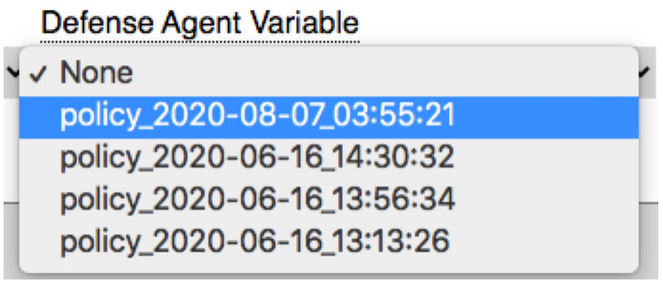
RL Control

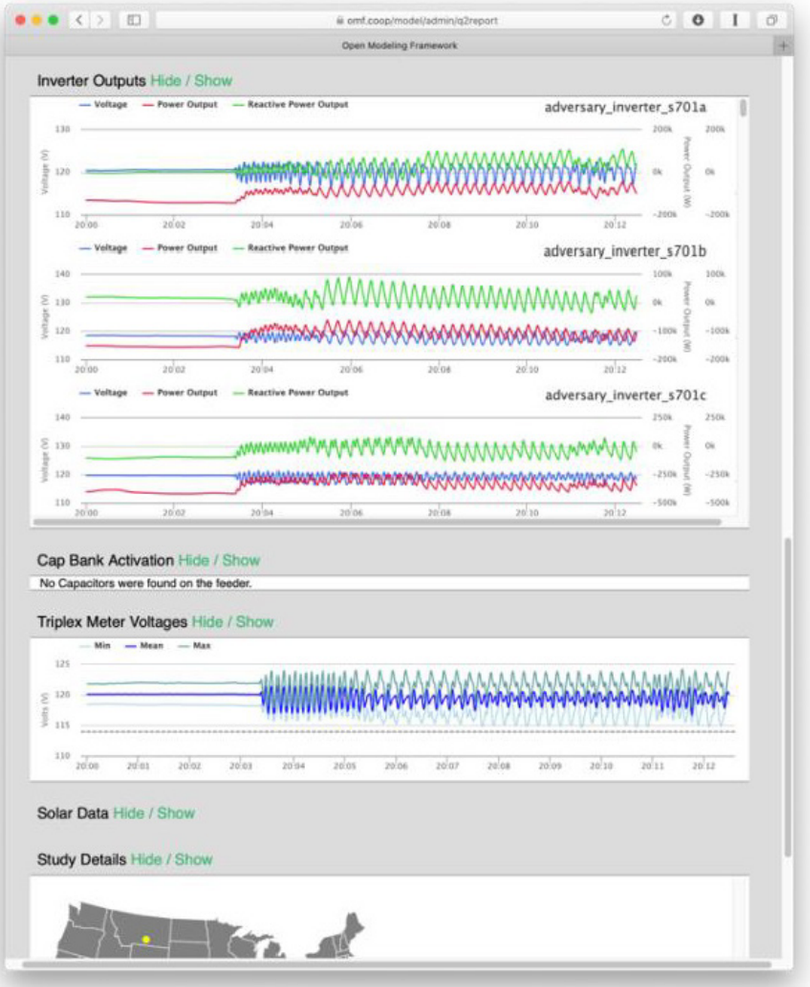


Paper accepted to SmartGridComm

Additional Slides – OMF Integration







Questions?