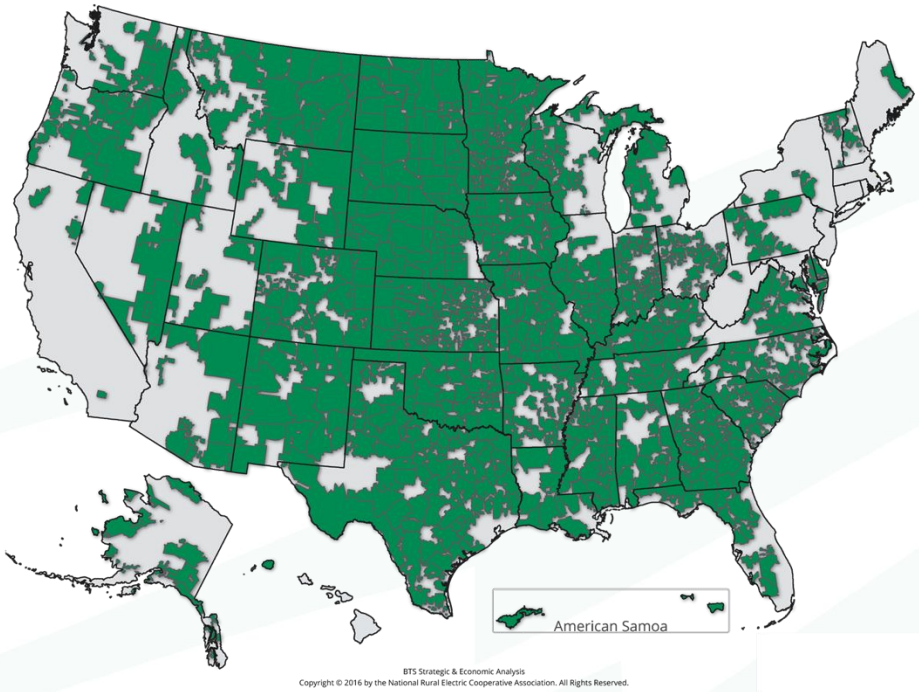
CIGAR: Utility Perspective and User Interface

david.pinney@nreca.coop, ryan.mahoney@nreca.coop, lisa.slaughter@nreca.coop

75 Years of Service
NRECA
America's Electric Cooperatives

March 17, 2021

America's Electric Cooperatives

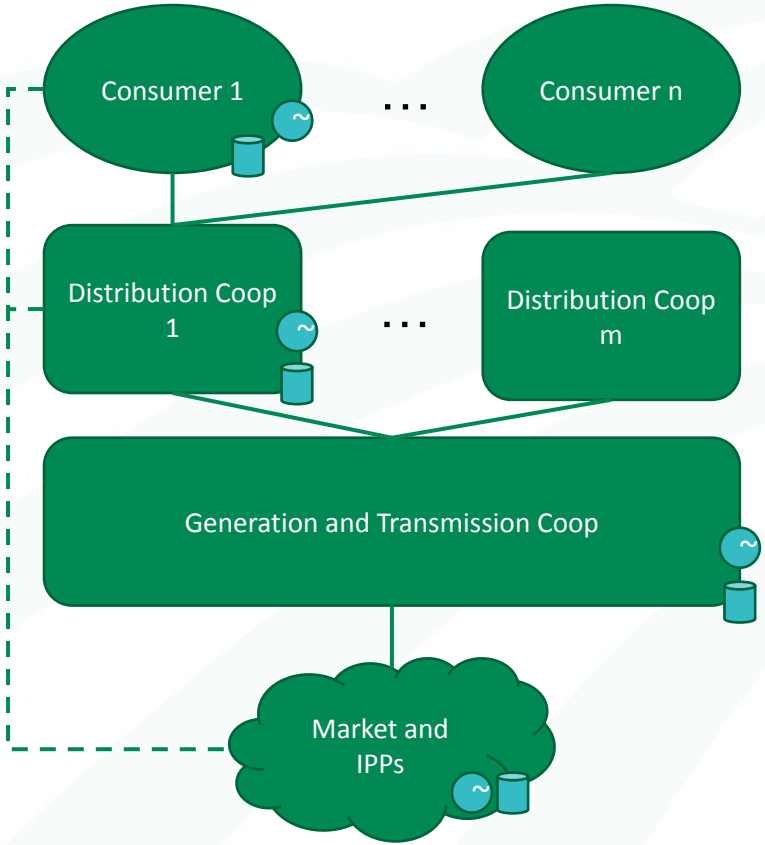


75 Years of Service
NRECA
America's Electric Cooperatives

- Serve 42 million people in 47 states through 65 generation & transmission (G&T) co-ops and 840 distribution co-ops
- Own and maintain 42% of the nation's distribution lines
- Average 7.4 consumers per mile of distribution line
- NRECA is a trade association serving the cooperatives through government relations, pension and healthcare services, research, etc.

Cooperative Power Supply Structure with Inverters

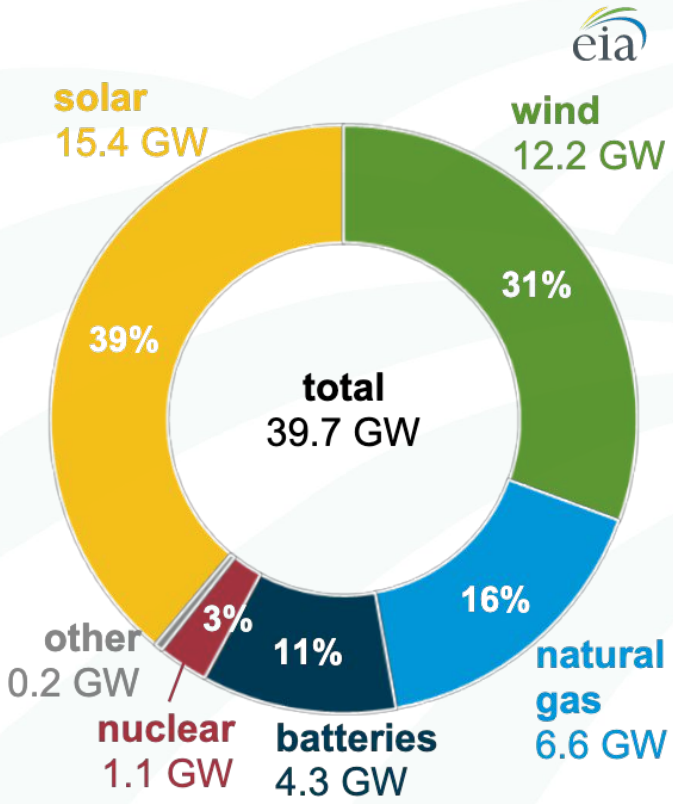
- Hierarchical supply system.
- DERs can go pretty much anywhere.
- Distribution coops typically limited to 5% DER production contractually, storage counting against this limit.
- ITC for solar + storage.
- Storage PPAs gaining popularity.
- Very rare for consumers and distribution coops to access IPPs and the market.
- Behind-the-meter: ideal deployment location?



75 Years of Service
NRECA
America's Electric Cooperatives

Motivation for DER Cybersecurity

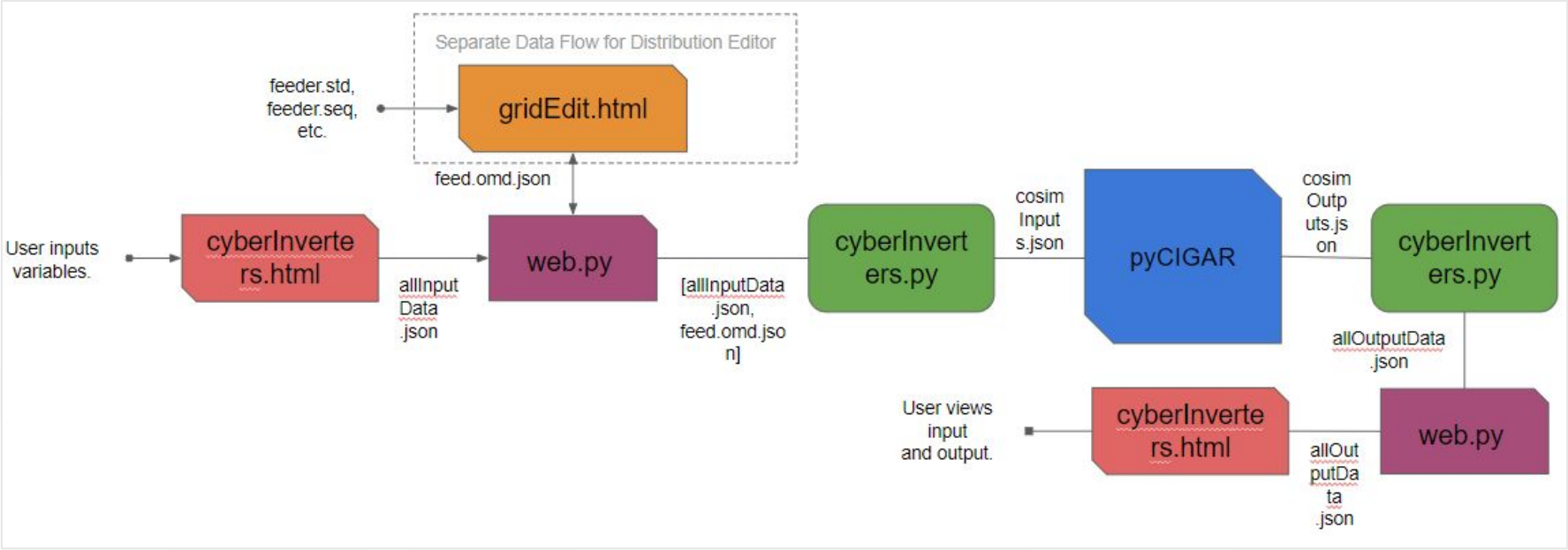
- Inverter Cyberattacks:
  - Demonstrated in the lab,
  - Executed on the grid,
  - Other nations have access to US infrastructure,
  - Large (800k) firmware updates becoming common
- IEEE1547: From 12 pages to over 100.
- Energy storage deployment and hence inverter deployment is growing +100% annually. EIA 2021 projected additions to right.
- When DERs are deployed we need to know:
  - What inverter settings could destabilize the distribution system for a given circuit.
  - Given a set of hacked devices, what control actions on non-hacked devices could mitigate the destabilizing behavior of the hacked devices.



75 Years of Service
NRECA
America's Electric Cooperatives

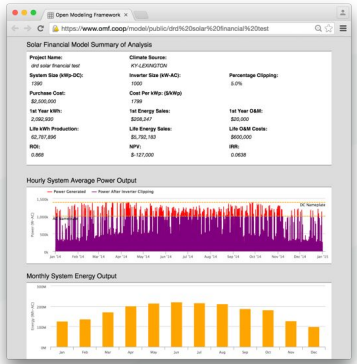
The PyCIGAR user interface: cyberInverters

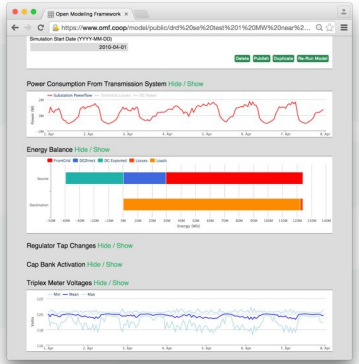
- cyberInverters: OMF.coop model that utilizes pycigar simulation tool to show the effects of different attack/defense agents on a distribution grid over a certain time period.
- Our key user: chief distribution planning engineer.

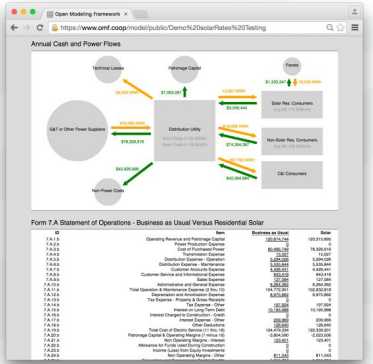


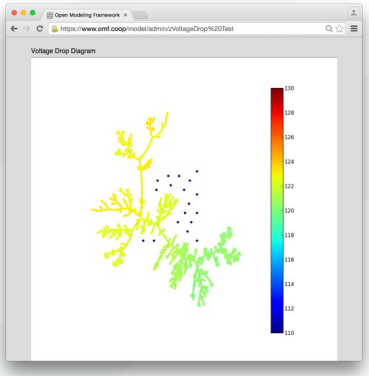
Framework Approach – https://OMF.coop

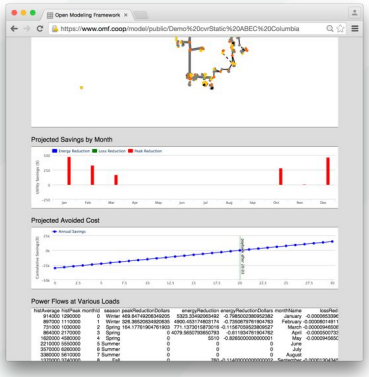
- Free and open source electric utility modeling software
- Built over the last 6 years by the co-ops and the US Department of Energy
- Python backend and support libraries, light web-based frontend
- Main focus: applications that perform financial and engineering analysis for utilities on emerging technologies (solar, energy storage, networked controls)
- Secondary focus: environment for researchers to develop new models
- Users from 217 organizations (utilities, vendors, universities) as of July 2019

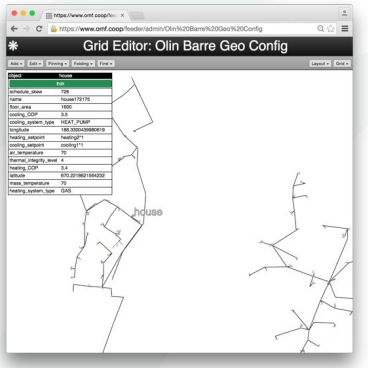








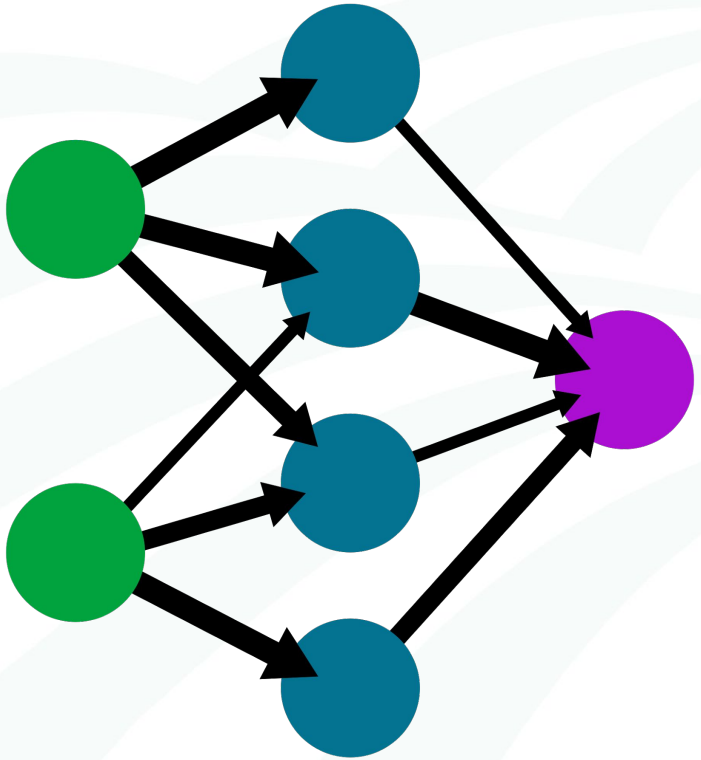




75 Years of Service
NRECA
America's Electric Cooperatives

Deep Reinforcement Learning

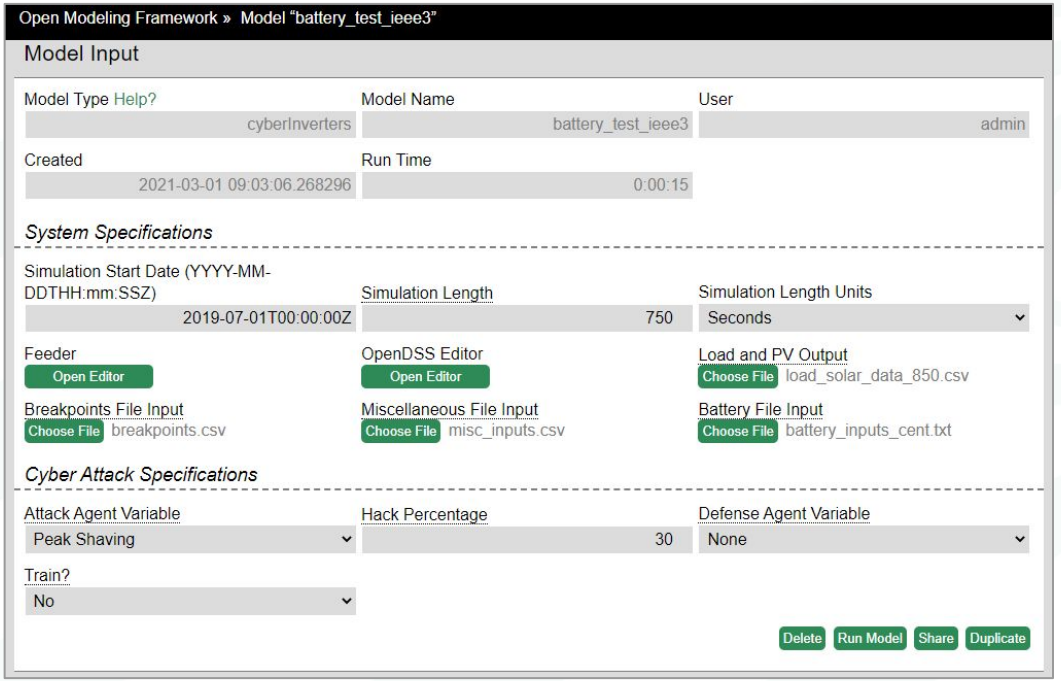
- Smart *agents* in LBL's pycigar control inverters in the simulation to intelligently counter malicious behavior of hacked devices.
- Agents gain their intelligence through training over millions of scenarios using *deep reinforcement learning*.
- Deep reinforcement learning has been hugely successful in other fields (super-human results in game playing, self-driving cars, facial recognition protein folding, etc.)
- Attacks can also be defined as agents to make training more rigorous (spy-versus-spy).



cyberInverters Model Inputs

"System Specifications" Section

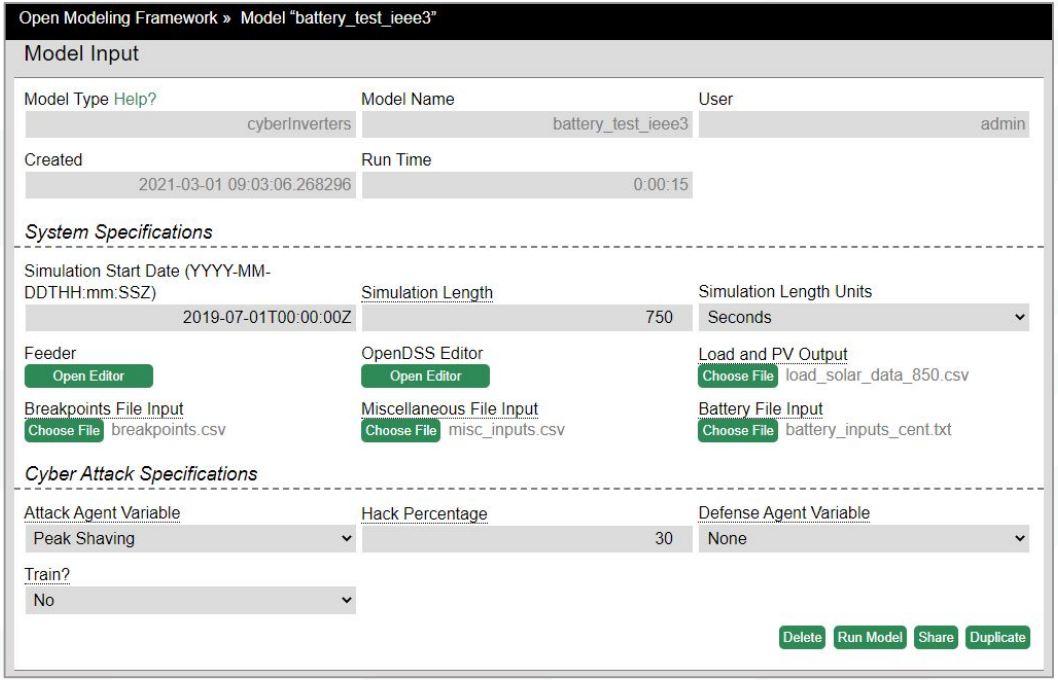
- **Simulation Start Date** - The date and time at which the simulation begins.
- **Simulation Length** and **Units** - The length of time the simulation will span and the associated units.
- **Feeder** - "Open Editor" button redirects user to a visual editor of the feeder circuit input.
- **OpenDSS Editor** - "Open Editor" button redirects user to a text editor of the .dss circuit definition file.
- **Load and PV Output** - Allows user to upload a .csv containing distributed load and solar generation data at each simulation timestep.
- **Breakpoints File Input** - Allows user to upload a .csv defining each inverter's volt-var curve.
- **Miscellaneous File Input** - Allows user to upload a file containing hyperparameter definitions for the pycigar tool.
- **Battery File Input** - Future functionality. Allows user to upload a .csv defining batteries at various loads.



cyberInverters Model Inputs

"Cyber Attack Specifications" Section:

- **Attack Agent Variable** - Allows selection of different predetermined attack agents that simulate an attack on the circuit.
  - None (Default)
  - Voltage Oscillation
  - Voltage Imbalance
- **Hack Percentage** - Limits attack agent penetration to a random subset of the inverters on the circuit.
- **Defense Agent Variable** - Allows selection of any existing pre-trained defense agents.
- **Train?** - Allows the user to create a defense agent that can be used against a specific attack.
  - Yes - Trains a new defense agent using selected simulation specifications.
  - Saved as a file within the OMF model directory.

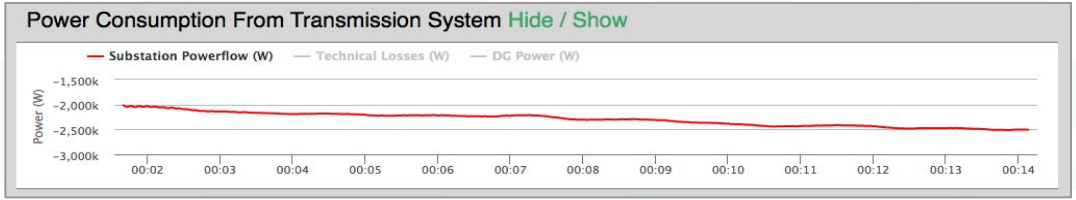


75 Years of Service
NRECA
America's Electric Cooperatives

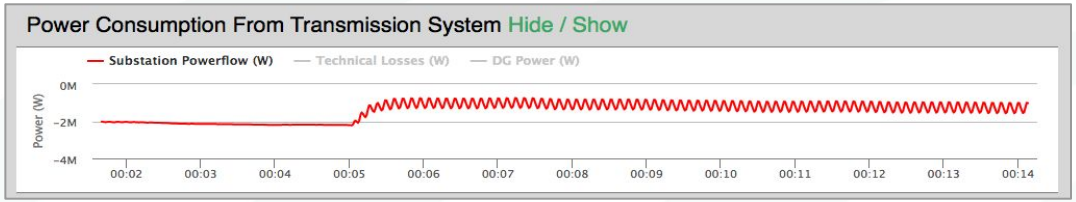
cyberInverters Outputs and Results

Power Consumption from Transmission System - Displays the impact of attack/defense on bulk power purchase and system losses over the simulation duration.

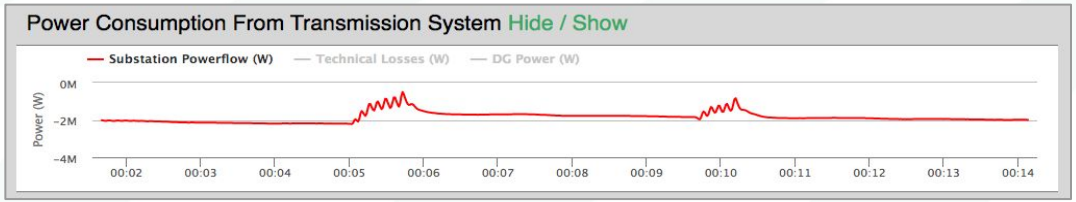
Control (No Attack or Defense) Scenario



Attack Scenario



Attack + Defense Scenario

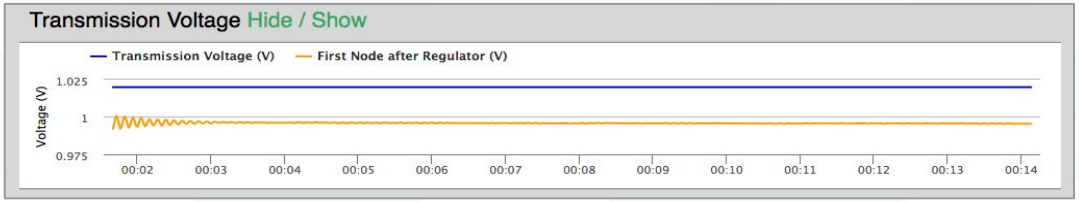


75 Years of Service
NRECA
America's Electric Cooperatives

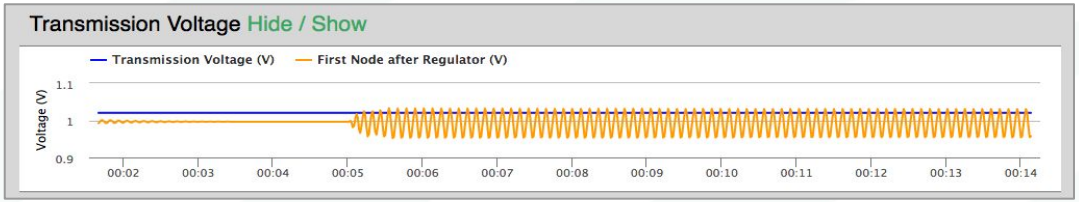
cyberInverters Outputs and Results

Transmission Voltage - Displays the transmission-level voltage and gives the user a clear representation of stability problems (if any) due to voltage regulator actions.

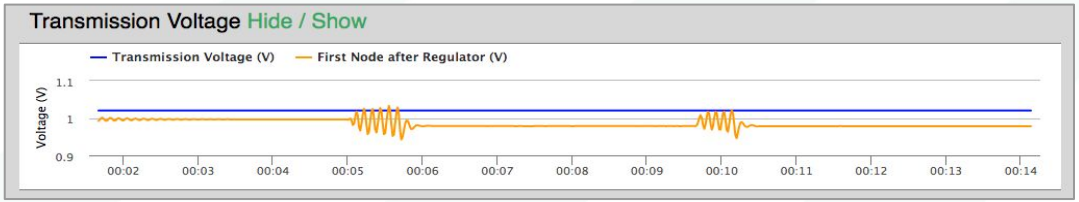
Control (No Attack or Defense) Scenario



Attack Scenario



Attack + Defense Scenario

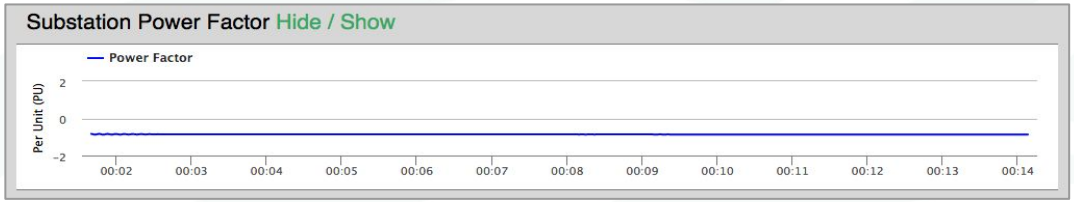


75 Years of Service
NRECA
America's Electric Cooperatives

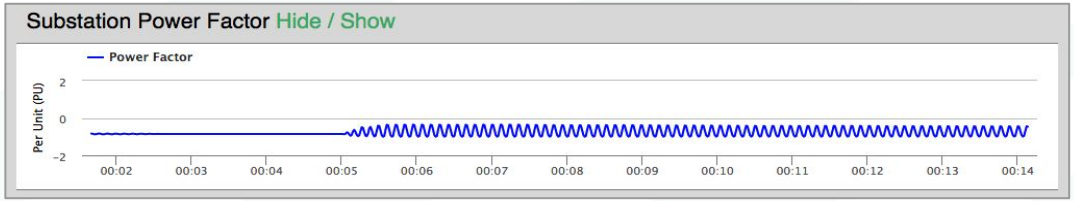
cyberInverters Outputs and Results

Substation Power Factor - Shows the effect of attack/defense agents on power factor at the head of feeder over the simulation duration.

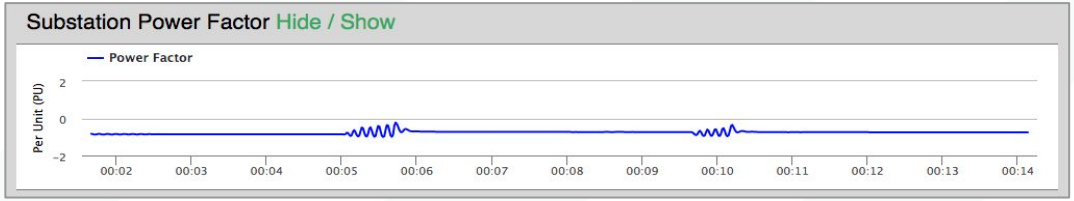
Control (No Attack or Defense) Scenario



Attack Scenario



Attack + Defense Scenario

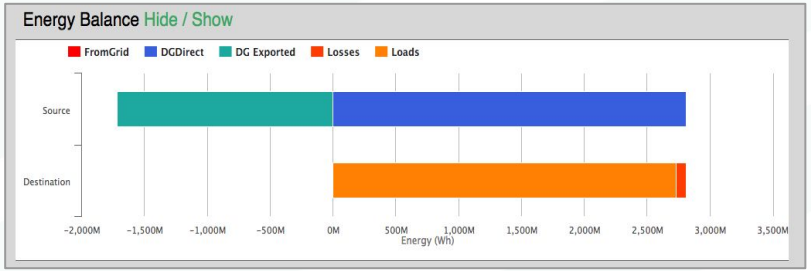


75 Years of Service
NRECA
America's Electric Cooperatives

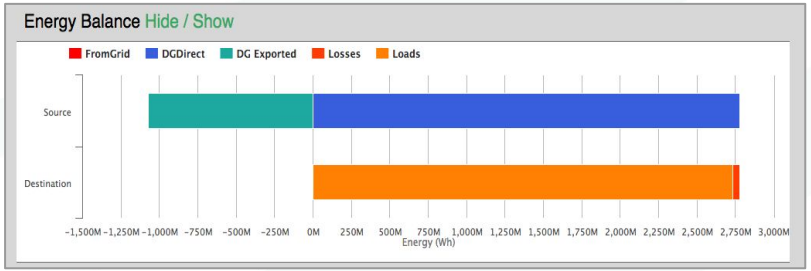
cyberInverters Outputs and Results

Energy Balance - Provides the user with a sanity check on total energy generation, consumption, and loss.

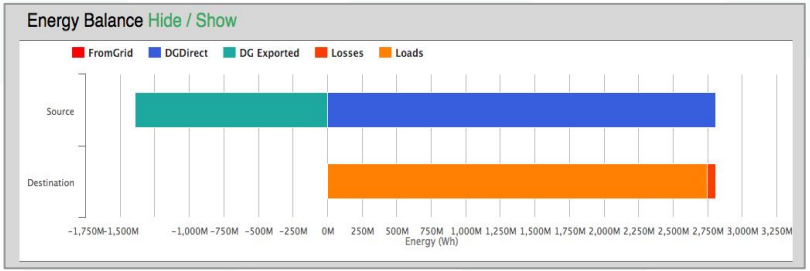
Control (No Attack or Defense) Scenario



Attack Scenario



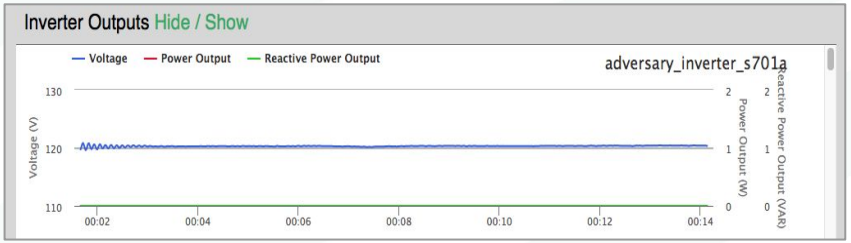
Attack + Defense Scenario



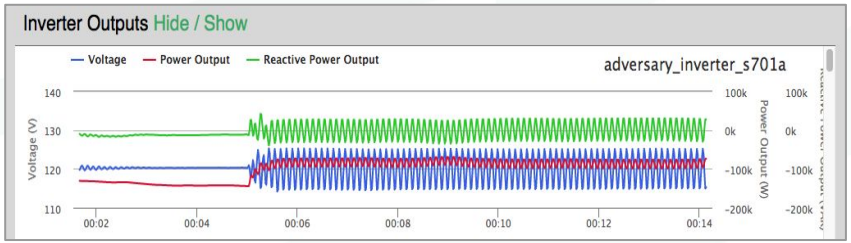
cyberInverters Outputs and Results

Inverter Outputs - Detailed graph for each inverter on the circuit showing the impacts of attack/defense agents over the simulation duration. The voltage readings, real power output, and imaginary power output are represented for each phase.

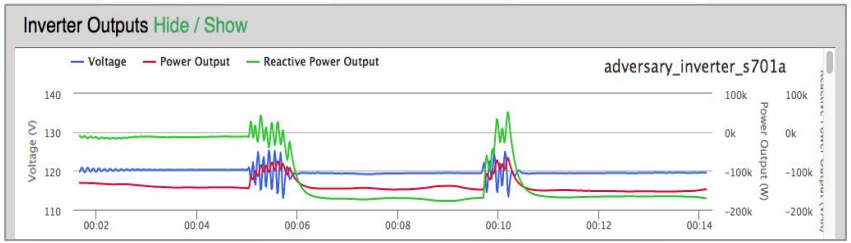
Control (No Attack or Defense) Scenario



Attack Scenario



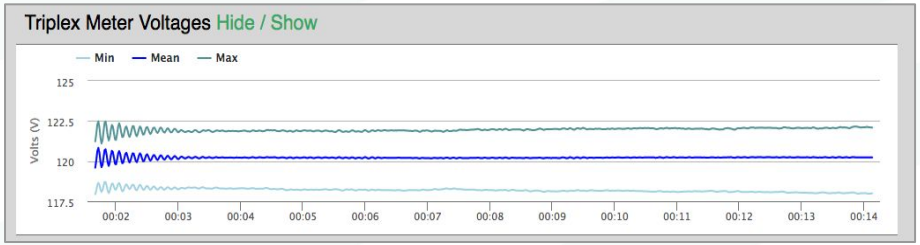
Attack + Defense Scenario



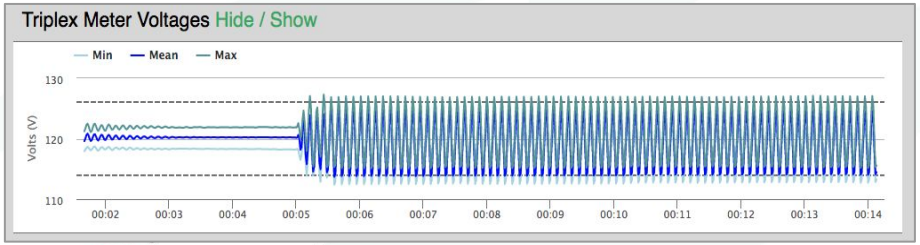
cyberInverters Outputs and Results

Triplex Meter Voltages - Shows the minimum, mean, and maximum voltages across all meters in circuit to give the user a representation of voltage abnormality.

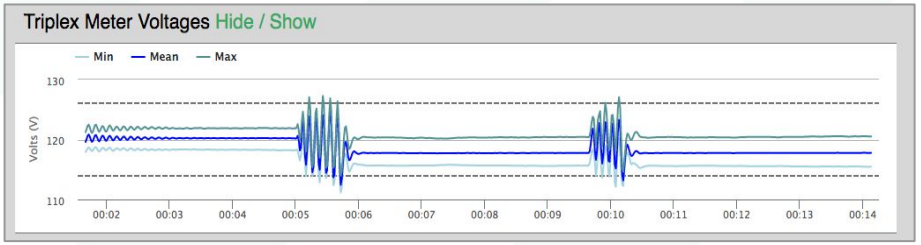
Control (No Attack or Defense) Scenario



Attack Scenario

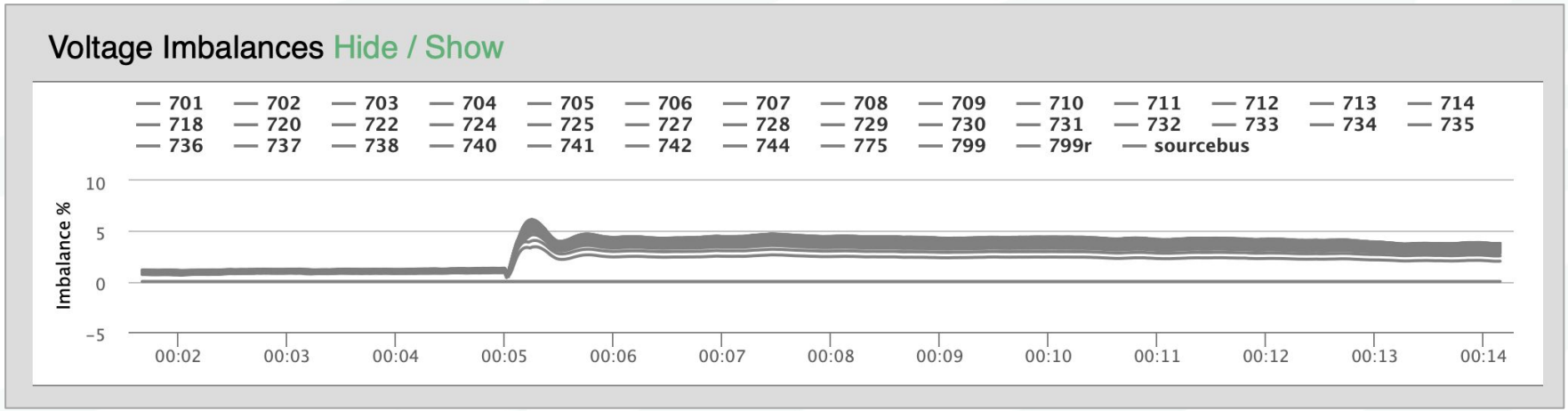


Attack + Defense Scenario



cyberInverters Outputs and Results

Other Outputs - include regulator tap changes, cap bank switching, and voltage imbalance to investigate second order effects.



75 Years of Service
NRECA
America's Electric Cooperatives

Next Steps with NRECA Research

- Detailed studies of realistic scenarios at cooperatives
- Enhanced energy storage simulation
- Electric Vehicle simulation

References

- Walton, R. (2019, November 4). *First cyberattack on solar, wind assets revealed widespread grid weaknesses, analysts say*. Utility Dive. https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/566505/
- Naylor, B. (2018, March 23). *Russia Hacked U.S. Power Grid — So What Will The Trump Administration Do About It?*. NPR. https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it
- Lee, R. (2016, March 18). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Electricity Information Sharing and Analysis Center. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
- Cybersecurity and Infrastructure Security Agency. (2018, March 15). *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors* (TA18-074A). https://us-cert.cisa.gov/ncas/alerts/TA18-074A
- Vijayan, J. (2007, September 28). Simulated attack points to vulnerable U.S. power infrastructure. Computerworld. https://www.computerworld.com/article/2541225/simulated-attack-points-to-vulnerable-u-s--power-infrastructure.html
- Roberts, C., Ngo, S., Milesi, A., Peisert, S., Arnold, D., Saha, S., Scaglione, A., Johnson, N., Kocheturov, A., & Fradkin, D. (2020). Deep Reinforcement Learning for DER Cyber-Attack Mitigation. ArXiv. abs/2009.13088.