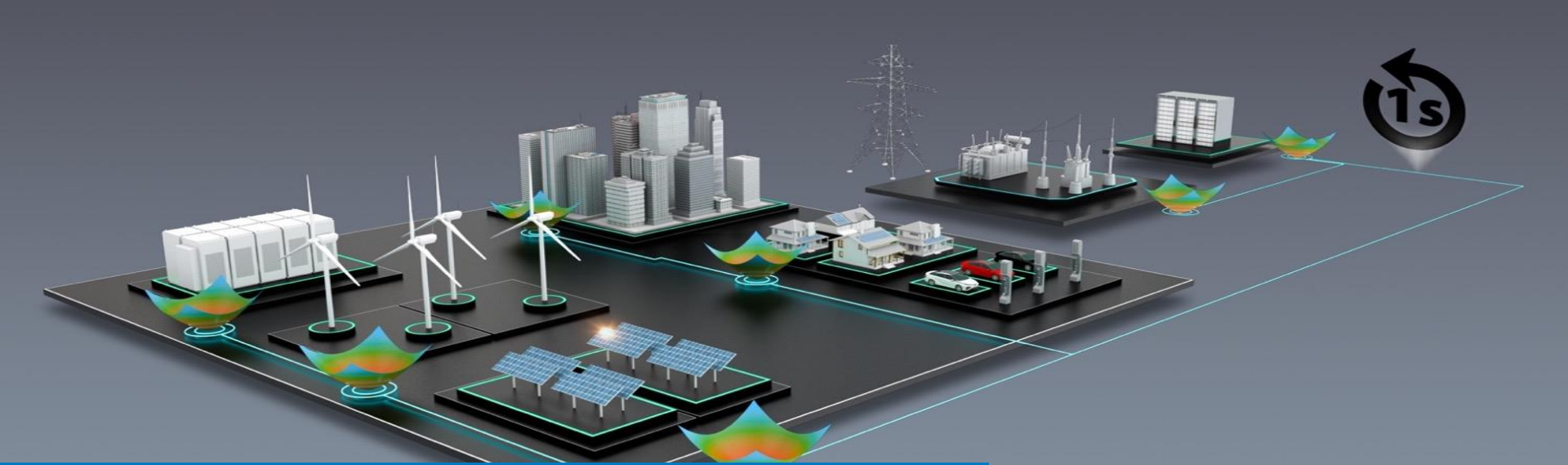
Situational Awareness of Grid Anomalies (SAGA)

Rui Yang, Michael Ingram, and Mengmeng Cai
Israel-U.S. Initiative on Cybersecurity Research and Development for Energy (ICRDE)

October 18, 2022

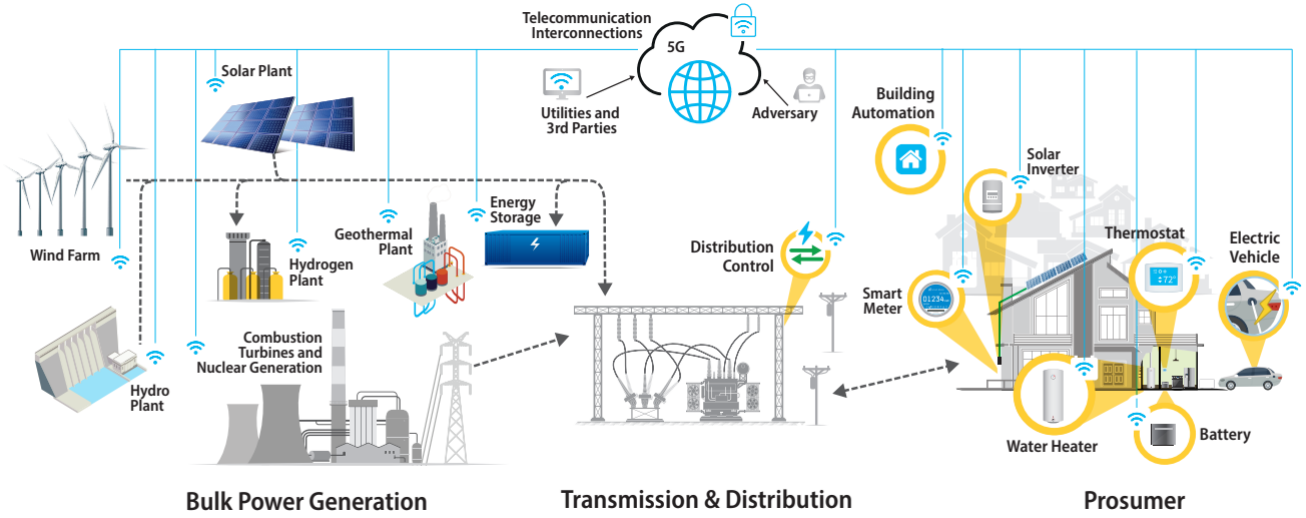
Photo from iStock-627281636



NREL's Power Systems Research

Conduct **high-impact research and development** (R&D) to solve the challenges of seamlessly integrating conventional and renewable sources, flexible loads, storage, and central and distributed generation, enabling resilient, reliable, flexible, secure, sustainable, and affordable power systems at all scales.

Cybersecurity for the Future Electric Grid



Technology Innovation

- Perform foundational R&D that integrates cybersecurity into the design of energy devices and systems
- Develop applications in electric vehicle (EV) charging and 5G communication networks.

Market and Planning

- Develop custom tools to support energy decision makers.
- Advance standards and share best practices.

Deployment Strategies

- Replicate cyber and physical characteristics of any system.
- Train, teach, and analyze organizations for cybersecurity deployment.

Outline

1. SAGA Overview
2. Cyber-Physical Co-Simulation Tool
3. Beyond Simulations—Linking With Hardware
4. Discussion

SAGA Overview

Presenter: Michael Ingram, NREL

Overview

Excerpts from proposals

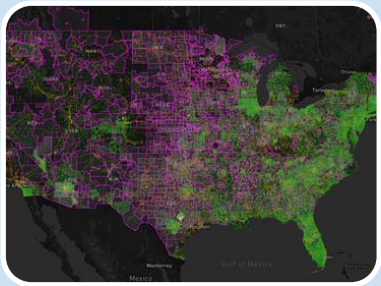
Image from iStock 479801072

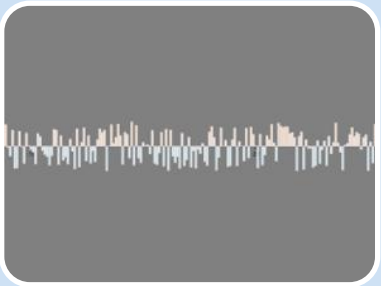
The Situational Awareness of Grid Anomalies (SAGA) project seeks to build upon foundational power system tools developed at NREL and integrate them with a growing set of data extracted from the Cable Television (CATV) broadband network infrastructure…to demonstrate a disruptive technology for power system data analytics relying on existing infrastructure.

To commercialize the rapid availability of grid voltage and phase angle data, this [TCF-20-20213] project developed the ANSI/SCTE standard 271 and created prototype broadband-based next-generation grid power sensors for use by utilities.

Overview

SAGA and Technology Commercialization Fund (TCF)





COLLECT:

- Preprocess
- Group data
- Publish application programming interface (API).

VISUALIZE:

- At multiple scales
- In high resolution
- Customizable views
- With anomalies highlighted.

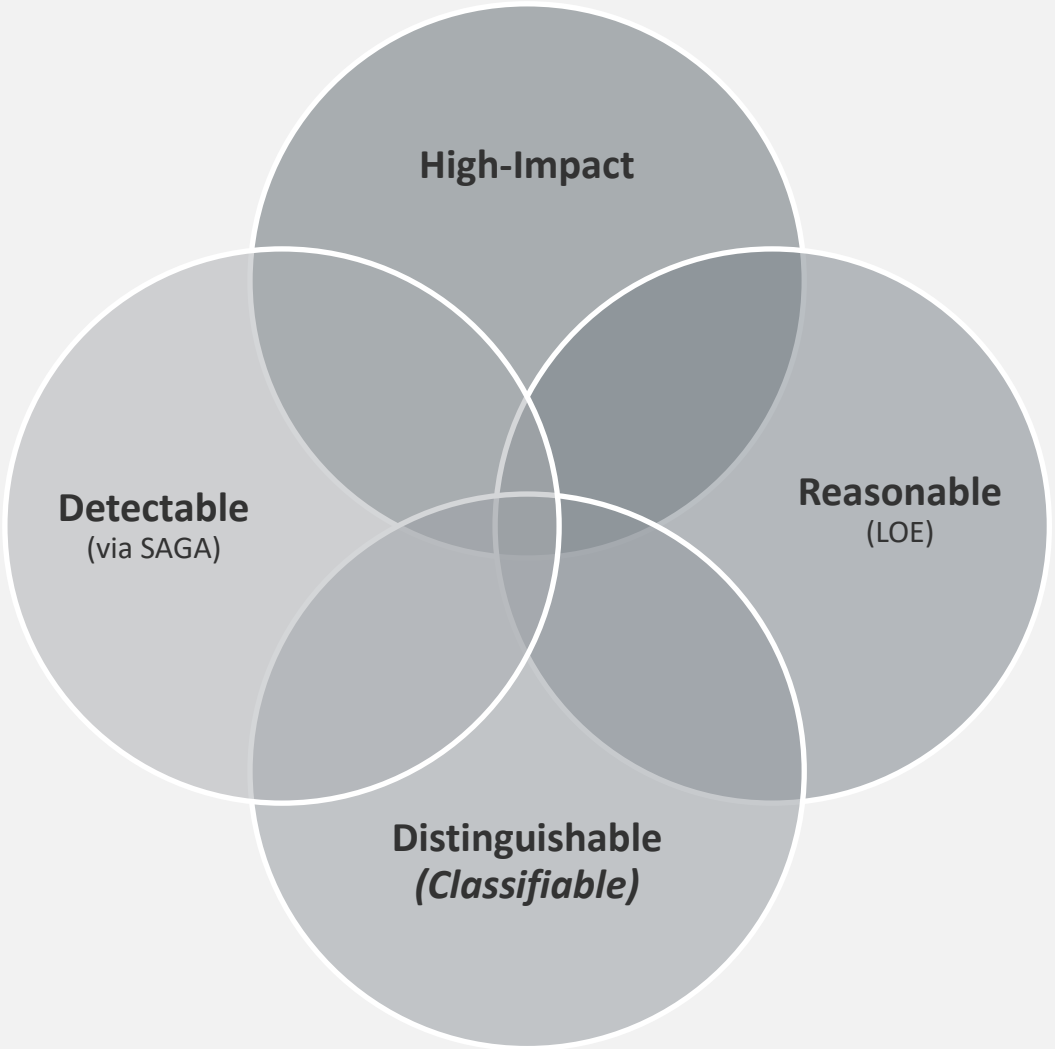
ANALYZE:

- For anomaly detection
- To support operations.

First research effort to apply CableLab's data to grid situational awareness

Cyber Use Cases

What makes a good use case?



IMPACTS

Grid instability

Injury/
loss of life

Economic impact

OBJECTIVES

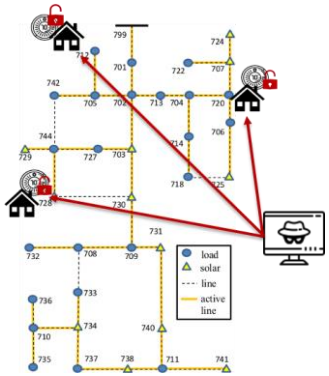
Voltage violations

Frequency
oscillations

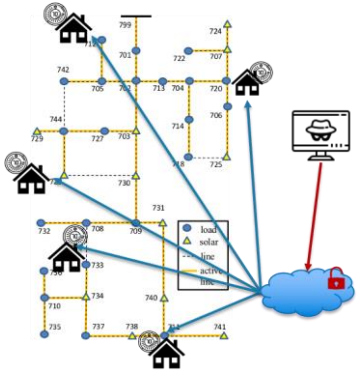
Safety violations

Inaccurate state
estimation

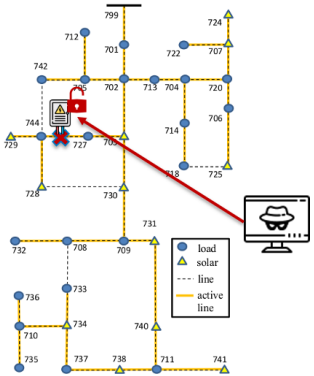
EVENTS



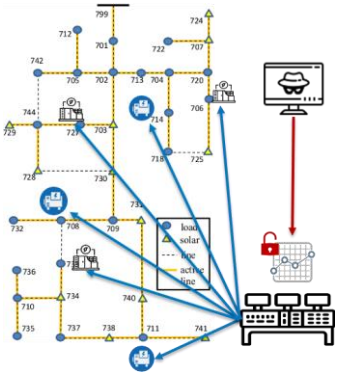
Smart home via Wi-Fi



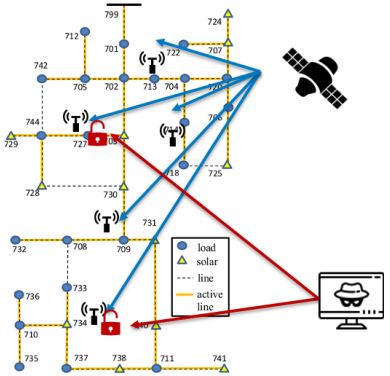
Smart home via cloud
(or firmware update)



Actuators



Control center



PMUs

DEVICES

1) Smart thermostats
2) EV chargers (home)
3) Batteries (home)

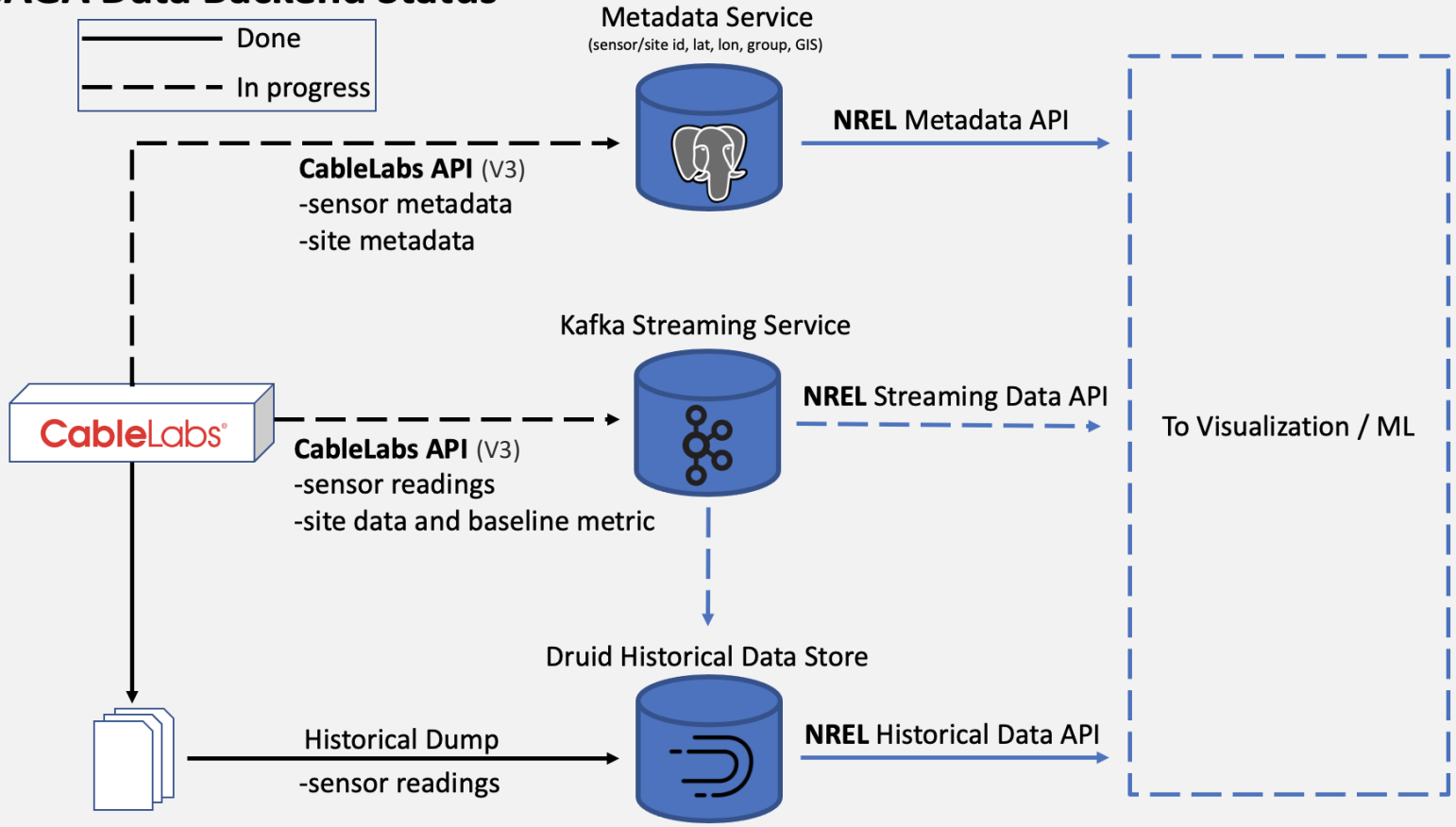
4) Load tap changer
5) Breaker/recloser

6) Distributed diesel gen
7) Batteries (utility scale)

8) PMUs

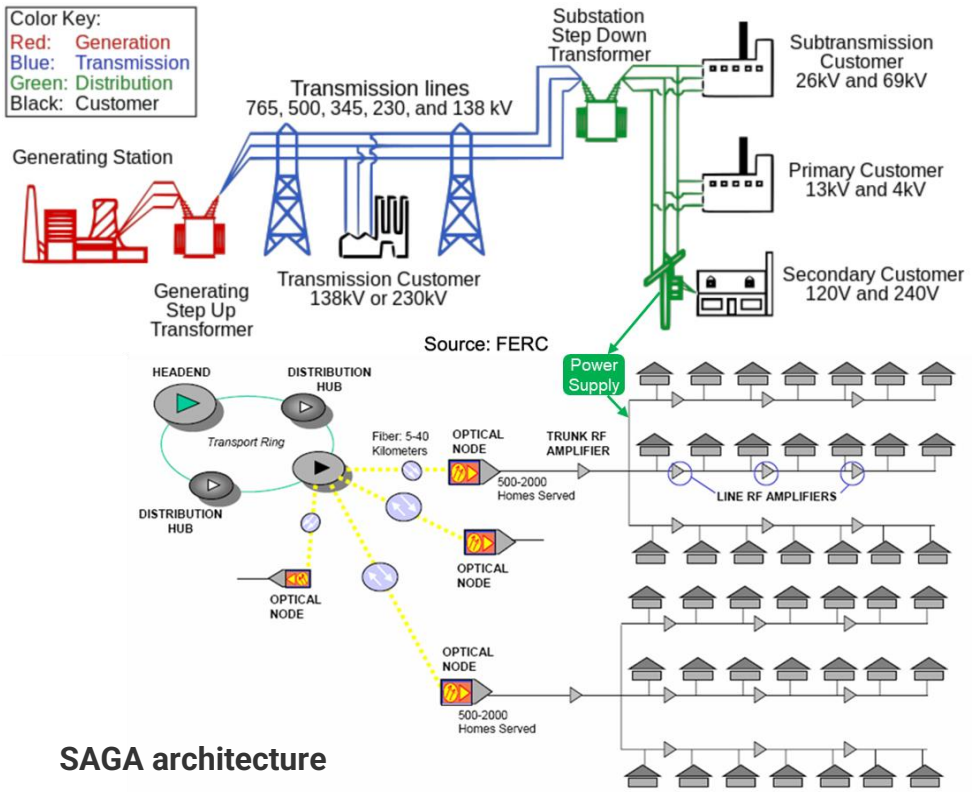
Data and Visualization

SAGA Data Backend Status



Accomplishments to Date

- 300,000+ sensors at year end:
  - 150 million in United States live within 1 km of a sensor.
- Identified states and scenarios:
  - Contextualized observations.
- Created sensor groupings:
  - Hospitals, airports, cities, states
  - Created baseline metrics by group.
- Modeled anomalous behavior
- Developed next-gen sensor:
  - 10,000 samples per second
  - Quarter-volt precision
  - ANSI/SCTE Std. 271 (2021) device.
- *Proposed "SAGA Ops":*
  - Doubling sensor footprint
  - Operationalizing data store.



SAGA architecture

Cyber-Physical Co-Simulation Tool

Presenter: Mengmeng Cai, NREL

Challenges and Objectives

➢ *Challenges*

New cyber vulnerabilities arise under the smart grid paradigm:

- The active role of distributed energy resources (DERs) opens the legacy grid control and automation systems to public communication networks.
- Heterogeneous network technologies and protocols
- Enhanced mutual impacts between transmission and distribution (T&D) systems.

➢ *Objectives*

To provide a scalable cyber-physical event simulation tool:

- T&D co-simulation
- Detailed DER dynamic model
- Computationally efficient (for supporting data-intensive cybersecurity relevant research).

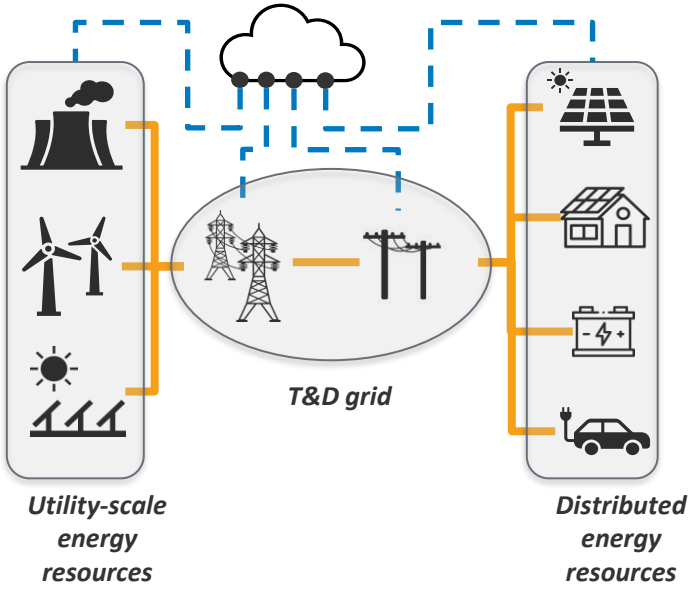


Figure 1. Smart grid paradigm with increased interconnectivity and interdependence

Modeling Approach

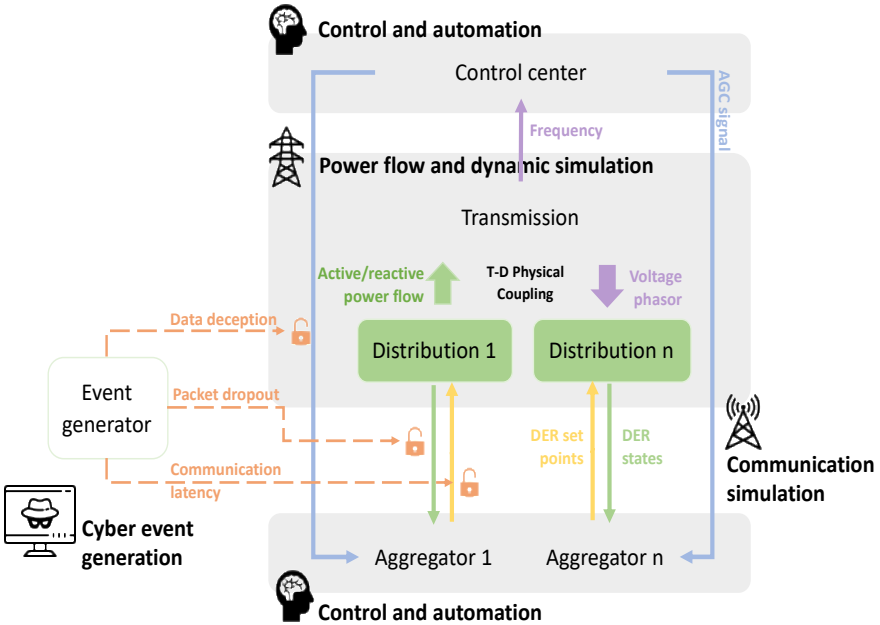
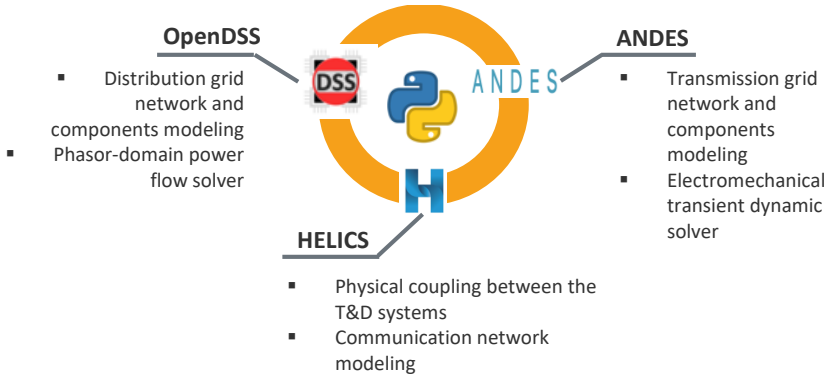


Figure 2. Framework of the SAGA cyber-physical co-simulation tool



- Federated co-simulation framework enabled by the Hierarchical Engine for Large-Scale Infrastructure Co-Simulation (HELICS)
- Physical values are exchanged via the HELICS publications and subscriptions (pubs/subs) interfaces.
- Messages (packetized data blocks) are exchanged via the HELICS end-point interfaces.
- Event metadata: event type, start time, end time, target feeder, target devices, and event magnitudes.

Distributed Energy Resource Modeling

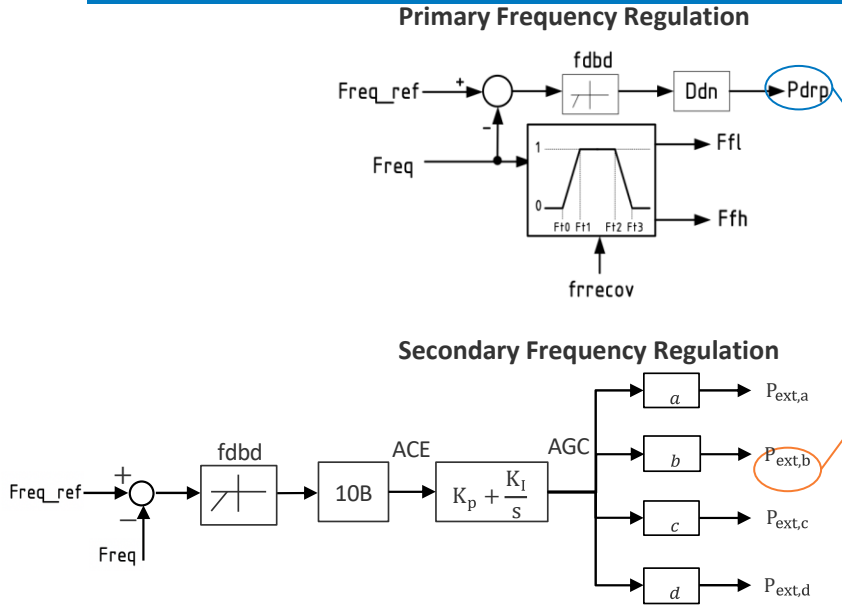


Figure 3. Frequency regulation control diagram

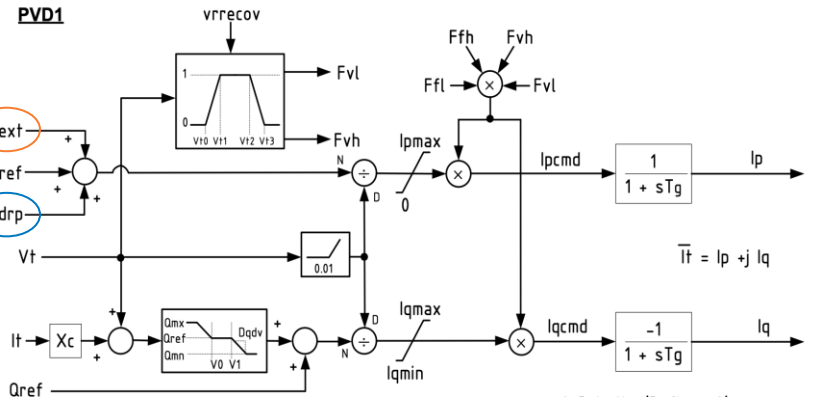


Figure 4. WECC PVD1 model

- The Western Electricity Coordinating Council (WECC) PVD1 model is applied to capture the DERs' fast dynamic response enabled by smart inverters.
- The primary frequency regulation, volt-volt ampere reactive (VAR) control, and protective generation tripping are enabled by the local controller.
- The secondary frequency regulation is performed by a centralized automatic generation control (AGC) model.

Cyber-Physical Events

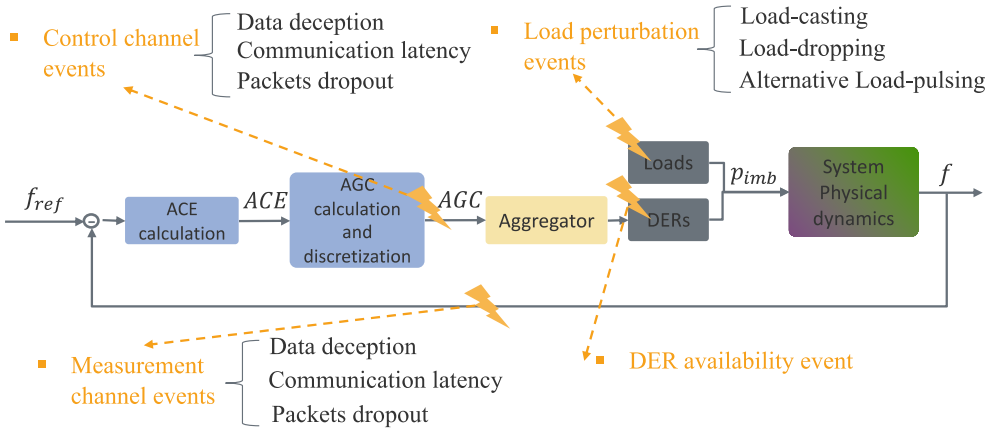


Figure 5. Illustration of the closed-loop AGC control and cyber-physical event entry points

- Load perturbation and DER availability events represent cyber-physical events targeting ***passive*** versus ***active*** system components.
- Three typical communication failures—data deception, communication latency, and packets dropout—are modeled.
- ***HELICS filters*** are applied to model the disruptions to communication links between the HELICS end points.

Case Study Setup

- **Test bed system:** connecting a 2,000-bus synthetic transmission network with 30 synthetic distribution networks (with more than 400,000 distribution nodes)
- **Load and generation capacity:** 67 GW (1.4 GW are modeled in detail at the distribution level) and 98 GW
- 6,000 **DERs** are modeled with a peak power generation of 199 MW and an installation capacity of 0.72 GW.
- All simulations are performed using high-performance computing (HPC) at NREL.

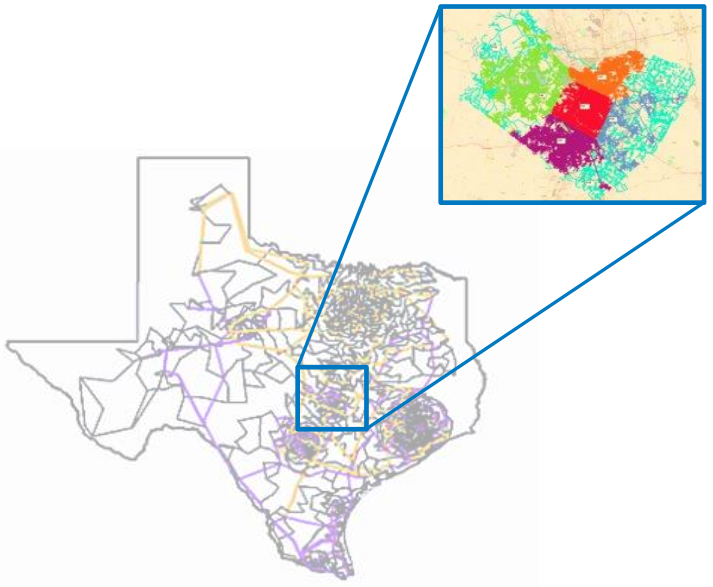


Figure 6. Footprint of the test bed system (a 2,000-bus synthetic transmission network connected with 30 synthetic distribution networks)

Load Perturbation Events

Load casting: $L_i(t) = L_i^0(t) + \alpha_i L_i^0(t), \forall i \in L_{target}$

Load dropping: $L_i(t) = L_i^0(t) - \beta_i L_i^0(t), \forall i \in L_{target}$

Alternating load pulsing:
$$L_i(t) = \begin{cases} L_i^0(t) + \alpha_i L_i^0(t), \text{if } t \in \tau[1,3,5,7,...] \\ L_i^0(t) - \beta_i L_i^0(t), \text{if } t \in \tau[2,4,6,8,...] \end{cases} \quad \forall i \in L_{target}$$

Table 1. Parameter Settings in Three Load Perturbation Events

	α	β	τ	Start Time	End Time
Load casting	U[0, 0.285]			8 s	38 s
Load dropping		U[0, 0.285]		8 s	38 s
Alternating load pulsing	U[0, 0.285]	U[0, 0.285]	3 s	8 s	38 s

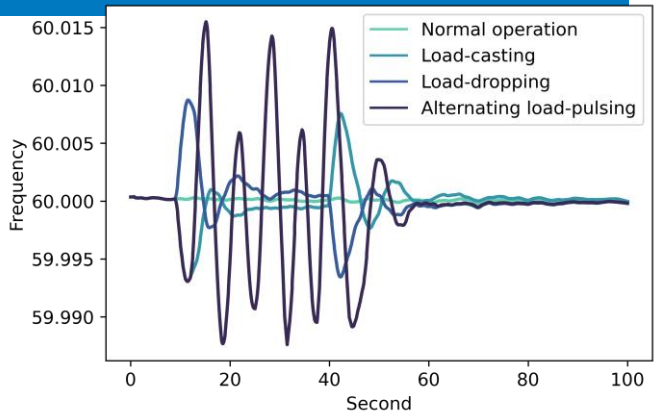


Figure 8. Frequency trajectories under different load perturbation events

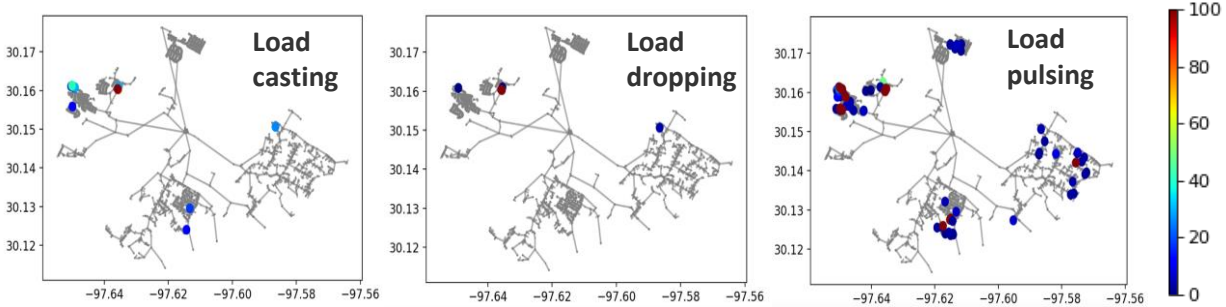


Figure 7. Durations of the voltage violations under three load perturbation events

- Alternating load-pulsing events could result in more significant frequency fluctuations and voltage violations despite the same level of attack cost.

Distributed Energy Resource Versus Load Relevant Events

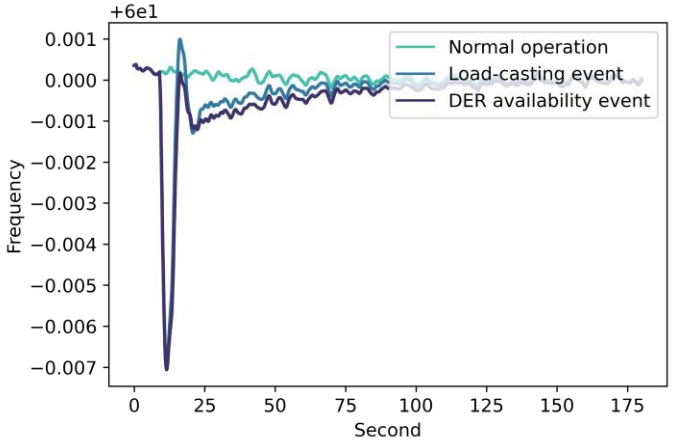


Figure 9. Frequency trajectories under load-casting versus DER availability events

Table 2. Frequency Recovery Time Under Load-Casting Versus DER Availability Events

	Load-Casting Event	**DER Availability Event**
Recovery time	66.3 s	113.3 s

- Both events cause an instantaneous 6.6-MW system demand surplus.
- The frequency nadirs under the two events are very close.
- The system frequency can recover and stay stable around its nominal value faster under the load-casting event than the DER availability event.
- The offline DERs are not responding to the AGC signals, which leads to a gap between the requested and delivered system AGC responses.

Synchronous Versus Asynchronous Communication Latency

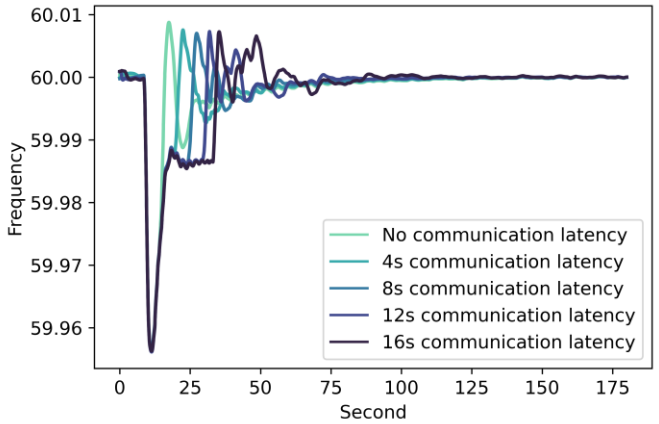


Figure 10. Frequency trajectories under different levels of synchronous communication latency

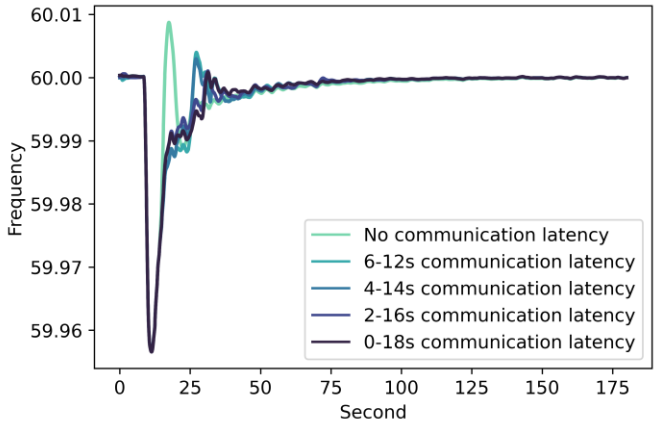


Figure 11. Frequency trajectories under different levels of asynchronous communication latency

- The greater the synchronous latency, the longer the frequency fluctuates before settling down.
- Synchronous communication latencies are more risky than asynchronous ones.
- Asynchronous communication latencies could even help suppress the frequency overshoot when the coefficients of the AGC PI controllers are well designed.

Measurement Channel Versus Control Channel Events

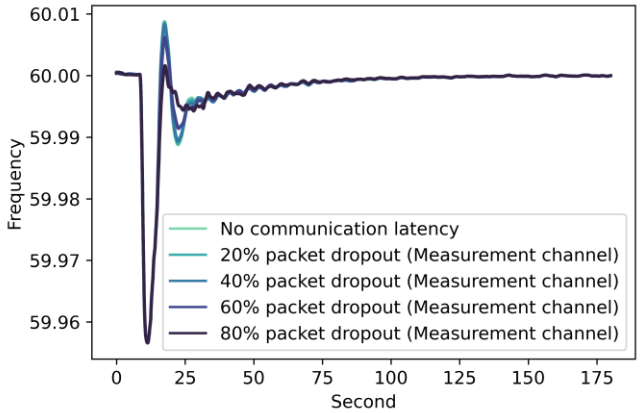


Figure 12. Frequency trajectories under different levels of packet dropouts occurring to the measurement channels

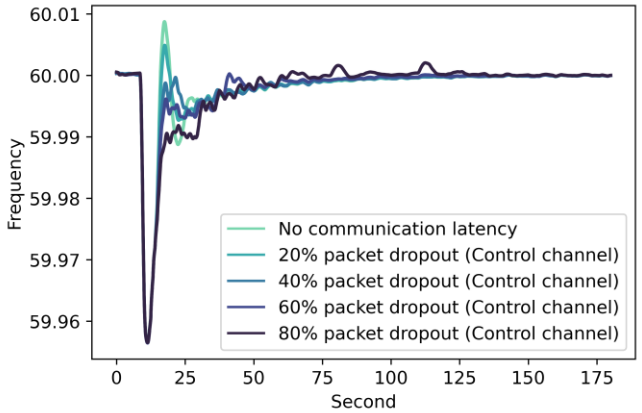
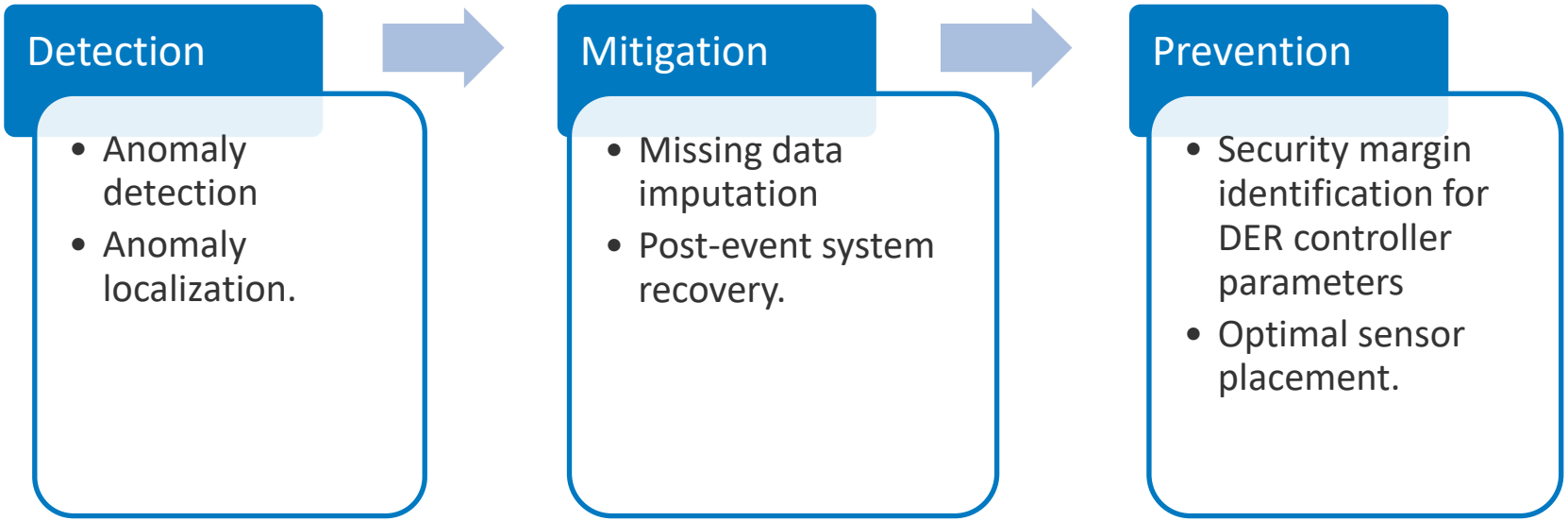


Figure 13. Frequency trajectories under different levels of packet dropouts occurring to the control channels

- The same frequency trajectories are obtained for the communication latency events no matter whether the cyber-physical event enters at the control channels or the measurement channels.
- The system impacts under the same dropout rate are more significant for events happening at the control channels than the measurement channels.

Applications and Future Work



Future work:

1. Integration with advanced communication network simulator, e.g., NS-3, to provide additional realism to the existing model
2. Integration with other grid service scenarios, e.g., voltage regulation.

Beyond Simulations—Linking With Hardware

Presenter: Rui Yang, NREL

Energy Systems Integration Facility (ESIF)

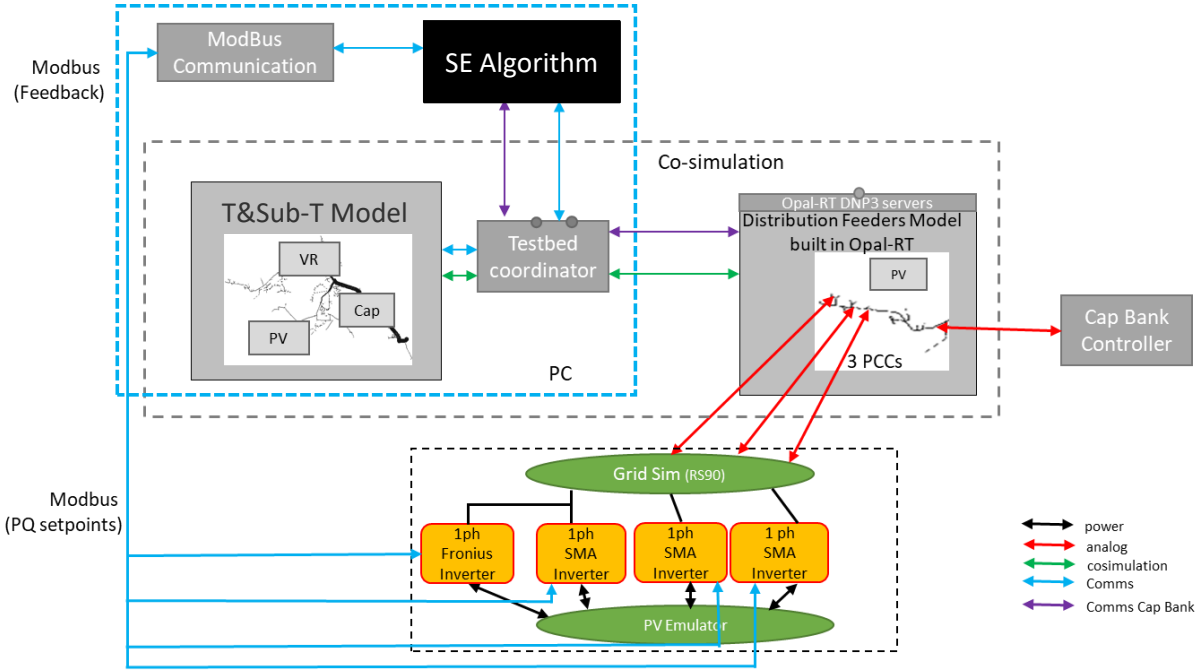
Shortening the time between innovation and practice

Unique capabilities:

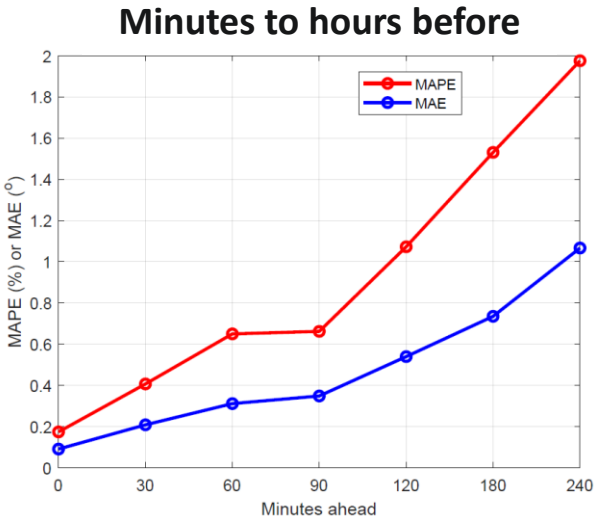
- Megawatt-scale power hardware-in-the-loop (HIL) simulation capability to evaluate grid scenarios with high penetrations of clean energy technologies
- Multiple parallel AC and DC experimental busses (megawatt power level) with grid simulation and loads
- Flexible interconnection points for electricity, thermal, and fuels
- Medium-voltage (15-kV) microgrid area
- Virtual utility operations center and visualization rooms
- Smart grid lab for advanced communications and control
- Interconnectivity to external field sites for data feeds and model validation
- Petascale HPC and data management system in showcase energy-efficient data center.

Hardware-in-the-Loop Demonstration: Situational Awareness

State estimation algorithm under cyber events



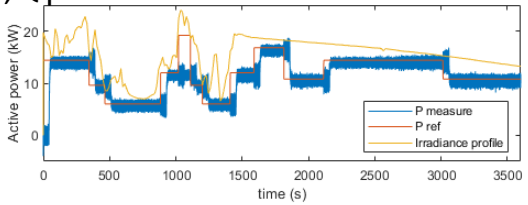
Replay attacks

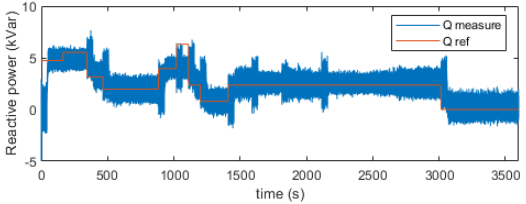


Hardware-in-the-Loop Demonstration: False Data Injection Attacks

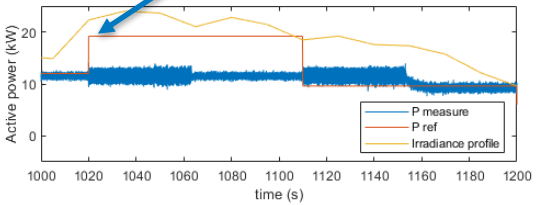
- Large-scale distributed system demonstration with false data injection (FDI) attacks on individual DERs
- Utility model running in phasor domain, photovoltaic (PV) inverter running in time domain
- PV inverter connected at one load bus:
  - Voltage and angle from the utility model used to create the grid voltage for inverter
  - Measured P and Q at the inverter terminal fed back to the phasor model.
- Man-in-the-middle attack:
  - Hacker manipulates set points of inverters.
- Perturbed the PQ set points (event based) sent to the devices and measured the output.

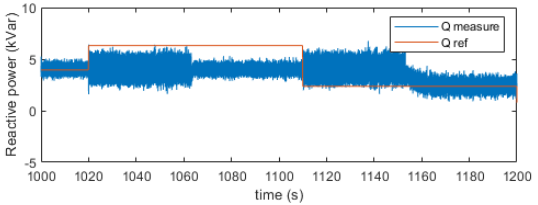
P,Q profile over the entire demonstration





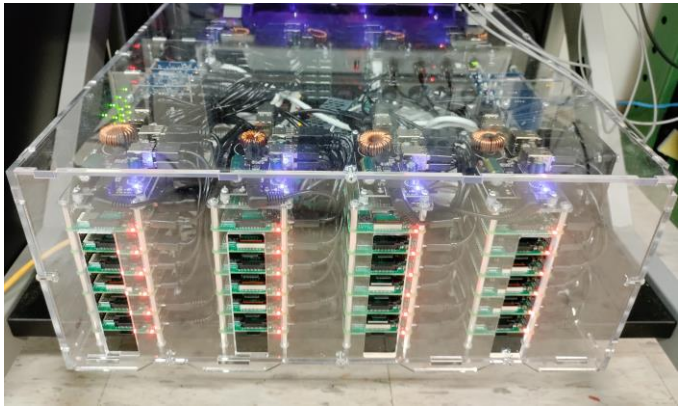
Malicious set point from hacker





Hardware-in-the-Loop Demonstration: Distributed Algorithms

- Distributed algorithms running on multiple physical devices (Raspberry PIs):
  - Consensus, optimization, state estimation, and others.
- Can simulate any communication topology and most protocols
- Data manipulation attacks:
  - Single or multiple nodes can be made to attack by changing the states shared with their neighbors.



Cluster with 48 Raspberry PIs

Thank you!

Contacts: Rui.Yang@nrel.gov
Michael.Ingram@nrel.gov
Mengmeng.Cai@nrel.gov

NREL/PR-5D00-84465

This work was authored in part by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Energy Efficiency and Renewable Energy. The views expressed do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.