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

Supervisory Parameter Adjustment for Distribution Energy Storage (SPADES)

Lawrence Berkeley Lab

Daniel Arnold

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

Project Overview

Objective

- SPADES uses Reinforcement Learning (RL) to defend Energy Storage Systems (ESS) from attacks targeting the ESS as well as the surrounding electric grid.

Schedule

- Jan. 1, 2020 – Dec. 31, 2022
- Task 1 - Feedback control modeling of ESS/electric grid interaction (in progress, due 12/31/2020)
- Task 2 – Supervisory control system development (due 12/21/2021)
- Task 3 - Red team experiment @ LBL FlexGRID facility (Fall 2022)
- Task 4 – Integration of RL agent into NRECA Open Modeling Framework (due 12/31/2022)

Total Value of Award:	**$ 3,209,749**
Funds Expended to Date:	**% 18.5**
Performer:	**Lawrence Berkeley National Lab**
Partners:	**Ariz. State University, Siemens CT, NRECA**

Advancing the State of the Art (SOA)

- (SOA) Current SOA for defending storage devices against cyber attacks does not utilize supervisory control to ensure internal states of ESS and the surrounding electric grid are protected from attacks
  - *Complexity of ESS power electronic controls makes ensuring internal stability difficult.*
  - *Stability issues arising from complex interaction between ESS and other systems in the grid have not been addressed.*
- (Feasibility) SPADES builds on CEDS project CIGAR and uses tools from adaptive control and reinforcement learning to adjust parameters in ESS control loops, taking into account other dynamics in the system.
  - *Adaptive control successfully used as parameter adjustment mechanism in other fields (aircraft control).*
  - *Reinforcement learning excels at deriving control policies in systems with complex interactions that are difficult to model explicitly.*

Advancing the State of the Art (SOA)

- (Pushing SOA) Adjusting ESS device parameters via adaptive control and RL allow ESS devices to “self-heal” and mitigates attacks caused by other compromised devices in the grid.
- (Benefit to End User) SPADES supervisory controllers could reside within ESS devices, allowing for immediate autonomous response. Utilities can use existing assets in their system to mitigate the effect of cyber attacks.
- (Advance CEDS) SPADES provides mechanisms for dynamically adjusting the behavior of ESS devices to maintain proper operation in the presence of attacks aimed at the ESS or the surrounding grid.
- (Adoption Potential) Task 4 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

- Task 1.1 - Literature survey of dynamic model of battery power electronic control systems. (Mar. 1, 2020)
- Task 1.2 - Developed feedback control model of ESS/electric grid interaction. Models characterized change of ESS state of charge as a function of active/reactive power injection or consumption, including battery inefficiencies and parasitic losses. (completed June 30, 2020)
- Go/No-Go: Successful development of 1 attack/defense use case for ESS control systems and DER-introduced voltage instabilities. (completed: June 30, 2020)
- Task 1.3, 1.4 - Storage use case development completed. Use cases based on NRECA member present and desired uses of storage. (e.g. peak shaving, capacity deferment) (completed: Sept. 30, 2020)
- Extremum Seeking (adaptive control technique) developed to dispatch power to mitigate instabilities caused by cyber attacks on solar photovoltaic smart inverter controllers. (journal publication planned)

Challenges to Success

Challenge 1 – Subcontracting Difficulties

- Subcontracting negotiations caused delay in project start.
- Mitigation: Risks mitigated by pushing back start date of project back to Jan. 1, 2020

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 will develop an adaptive control approach to adjust ESS parameters to maintain internal stability and ensure proper operation of the ESS in providing grid services. The adaptive controller will serve as a baseline for comparison in RL agent training.

Challenge 3 – Encouraging Utility Adoption

- Need to ensure developed algorithms will ensure proper ESS operation for wide variety of grid services (T&D deferral, peak shaving, etc.).
- Mitigation: Train RL algorithms for variety of ESS use cases. Ensure RL agents are stable for wide variety of network topologies.

Collaboration/Sector Adoption

Plans to transfer technology/knowledge to end user

- SPADES is beneficial for energy companies, vendors, researchers.
  - Utilities can simulate the effect of cyber attacks on ESS devices and the surrounding grid and use RL agents to test defensive strategies. This could lead to system hardening decisions (e.g. choosing "cyber-resilient" default parameters for ESS control functions).
  - DER vendors can integrate the defensive agent neural networks onto their devices to allow non-hacked units to directly participate in cyber-attack mitigation.
  - Researchers can use the SPADES framework to optimize distribution grids/microgrids 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 SPADES technology in a familiar tool.
- Red team experiments will be conducted in Fall 2022 at LBL's FlexGrid facility.
- NRECA/LBL will hold an end of project workshop to demonstrate technology to co-ops.

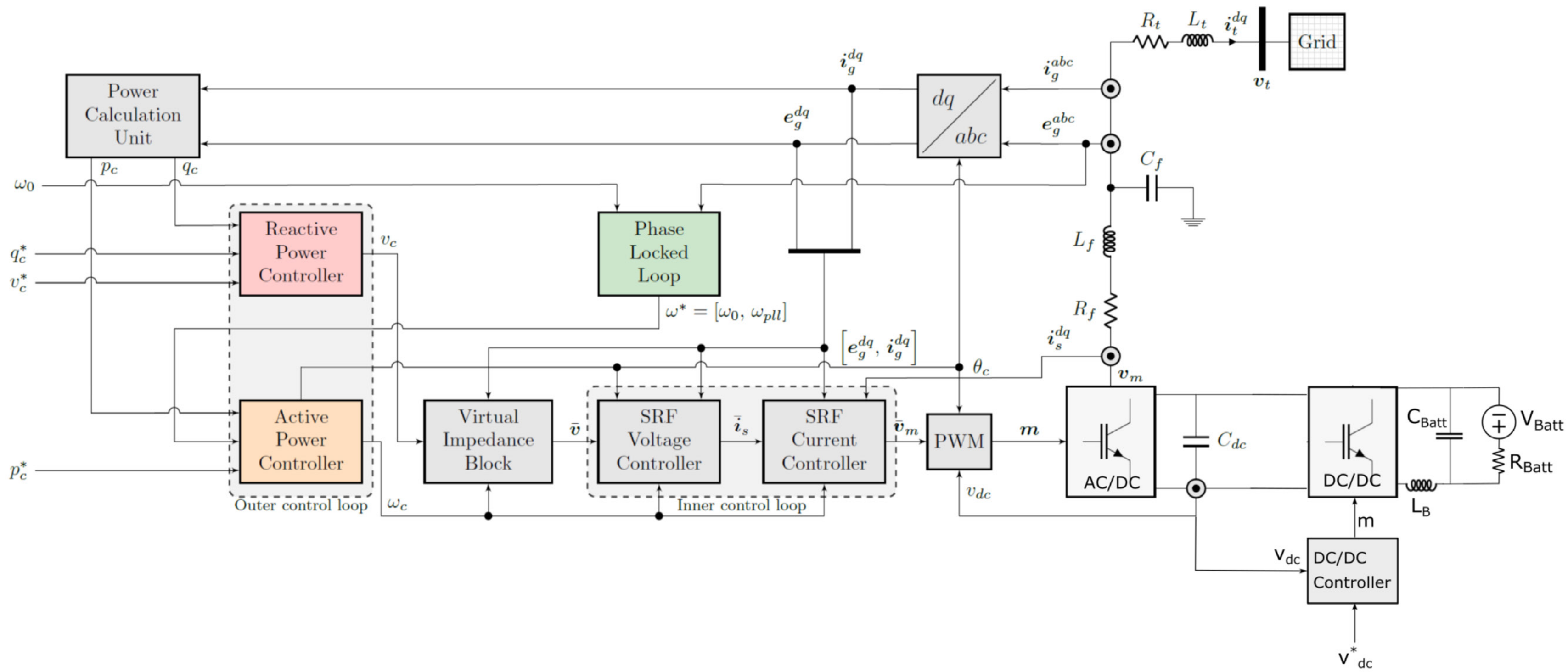
Next Steps for this Project

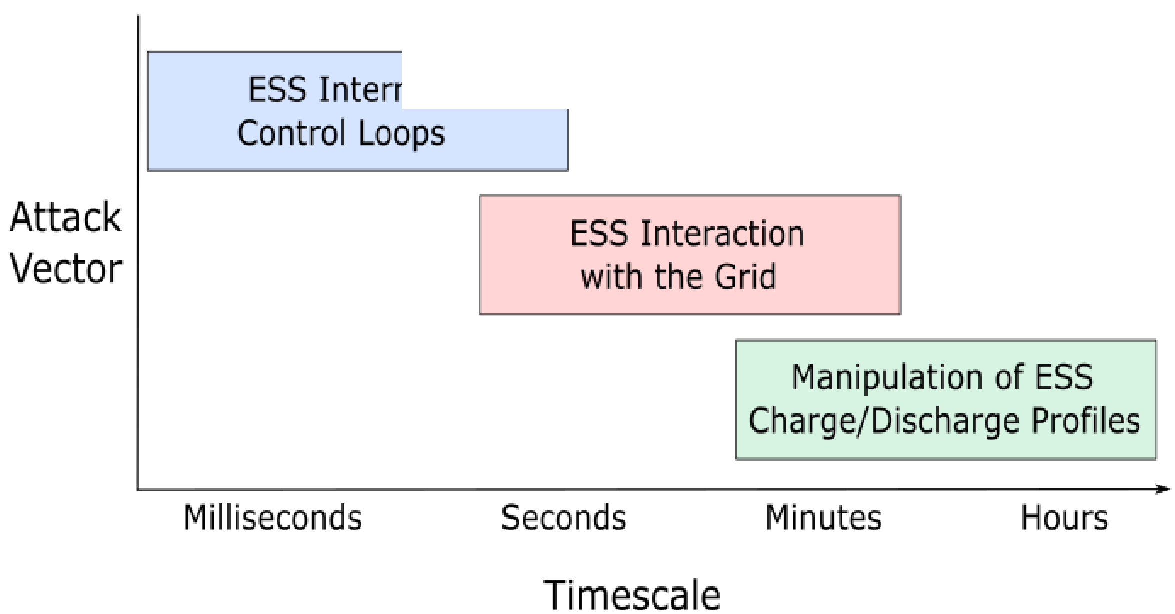
Approach for the next year or to the end of project

- Key Milestones:
  - Complete Task 1 - Feedback control modeling of battery/grid and simulation capabilities complete. (12/31/2020)
  - Complete Task 2 – Adaptive control/Reinforcement learning algorithm development complete, including software implementation. (12/31/2021)
  - Complete Task 3 - Red team experiment @ LBL FlexGRID facility. (09/30/2022)
  - Complete Task 4 – Integration the defensive reinforcement learning-based agent into the NRECA Open Modeling Framework (OMF) simulation tool. (12/31/2022)
    - Once this feature has been incorporated as a module into the OMF, utility users will have the ability to upload their network models, choose a desired ESS mode of operation, and conduct simulations to train specific instances of the defensive agent to defend against user-selected cyberattacks.
- Upcoming significant events:
  - Workshop with project partners and utility advisory board on feedback control modeling. (Dec. 2020)

Additional Slides - Motivation

Complexity of ESS control systems makes ensuring stability difficult



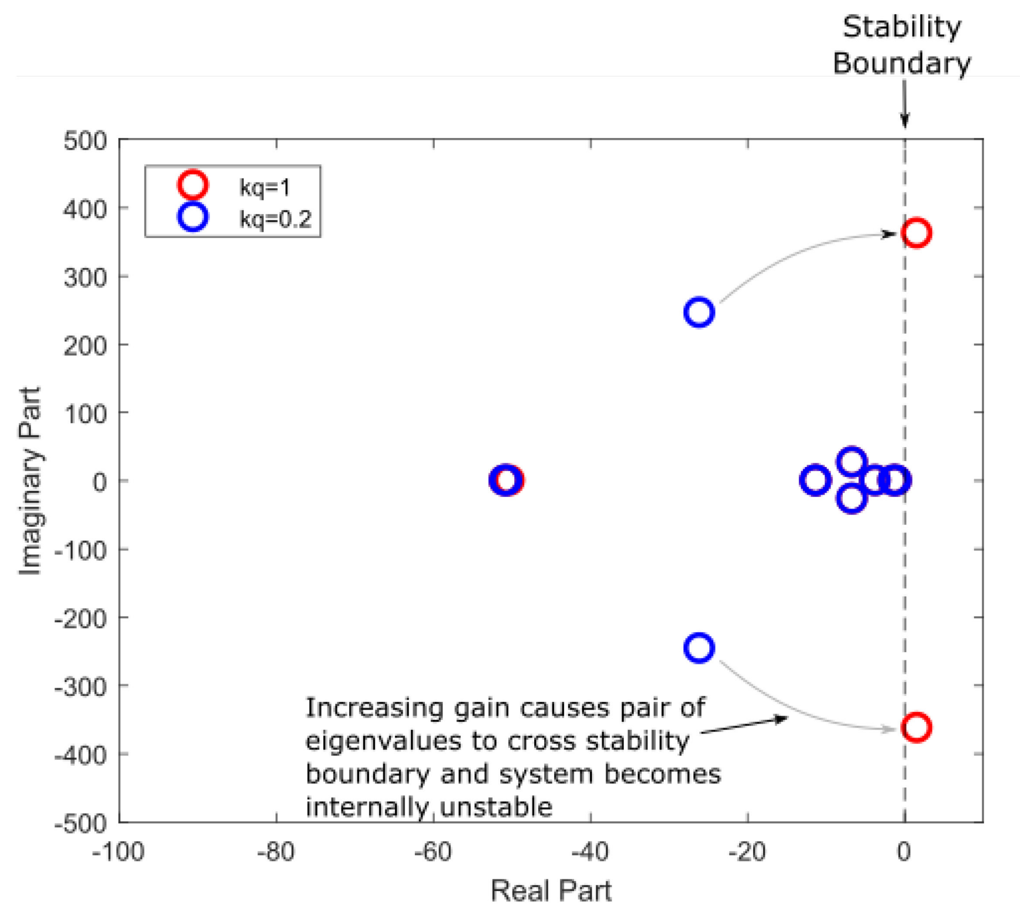


Threats to ESS/electric grid exist across multiple timescales

Additional Slides – Problem Definition

Cyberattack on ESS Control Parameters

- *Adversary accesses the registry of the converter firmware and changes a controller gain value.*
- *This change causes the current operating point to become an unstable operating point.*

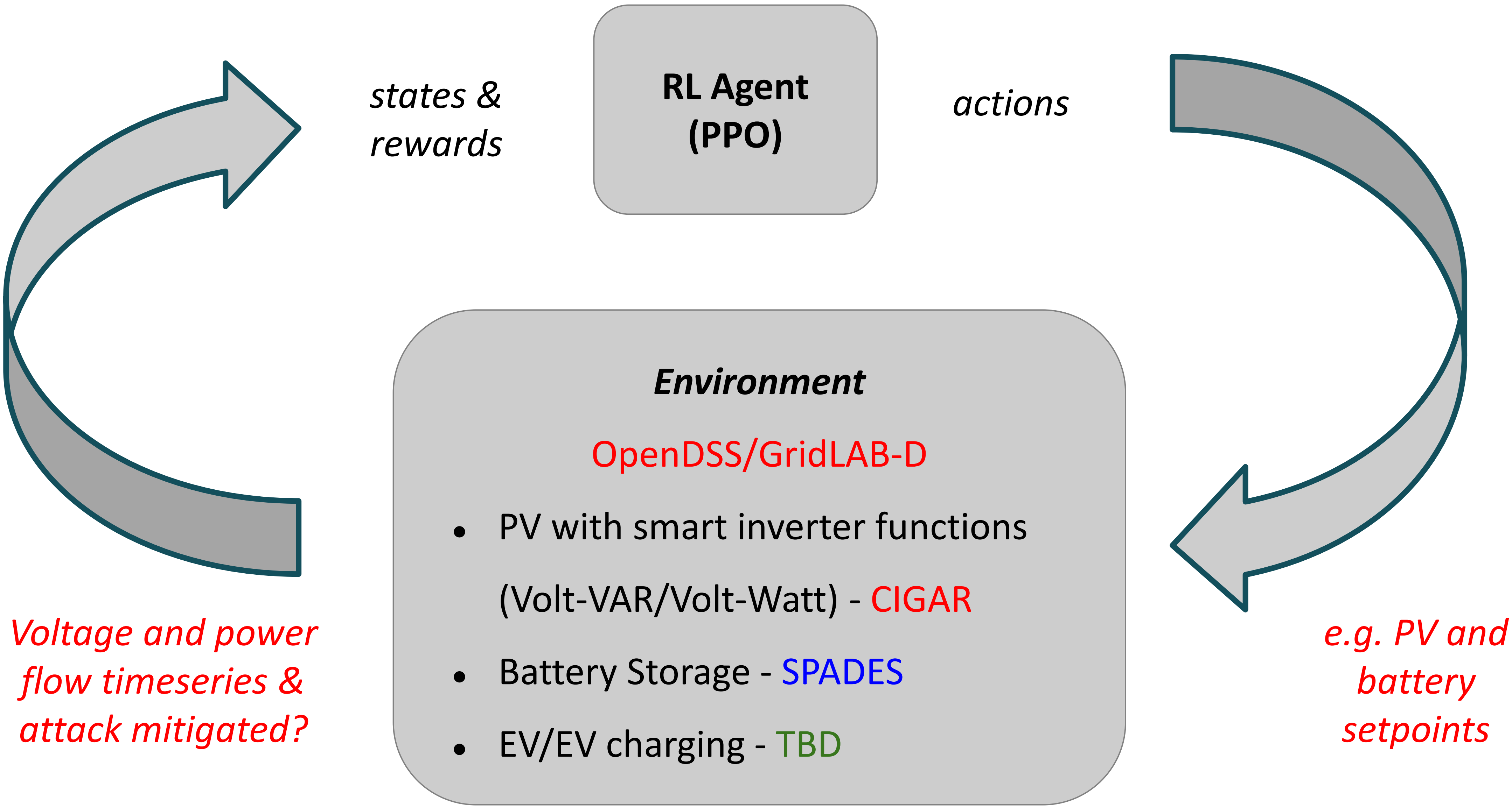


SPADES

- Defends ESS devices by adjusting internal control parameters.
- Defends the grid by adjusting settings in *non-compromised* units to mitigate cyber attacks on other distributed energy resources or ESS.

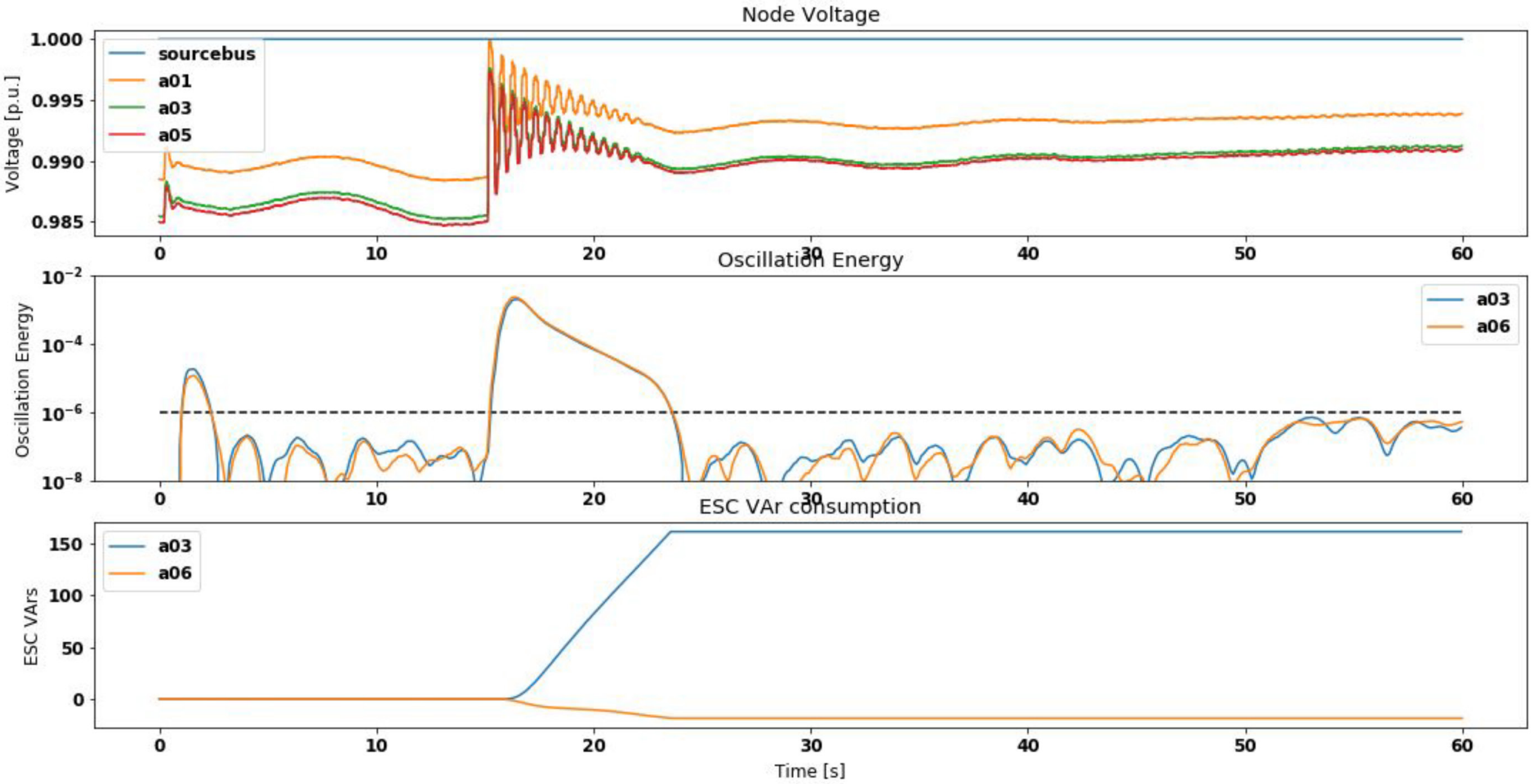
Additional Slides – Reinf. Learning

RL enables a holistic defense across different device types



Additional Slides – Preliminary Results

Use of ESS to mitigate instabilities in the grid



Extremum Seeking adaptive control of ESS power output

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

Additional Slides – Co-op use cases

Survey of most popular use cases for storage for co-ops

1. **T&D expansion deferral** - defer transmission line or substation transformer install/upgrade.
2. **Peak shaving** - reduce short-lived (< 4 hr) peaks in demand.
3. **Backup power / grid expansion** - provide power when the grid is unable to do so because of extenuating circumstance or prohibitive cost.
4. **Renewables firming** - balance short-term holes in generation due to intermittency of renewables.
5. **Islanded load and generation balancing** - balance microgrid intermittent generation with load on a fast time scale.

Next steps involve incorporating control loops that govern storage to provide these services into simulation environment for RL agent training.

Questions?