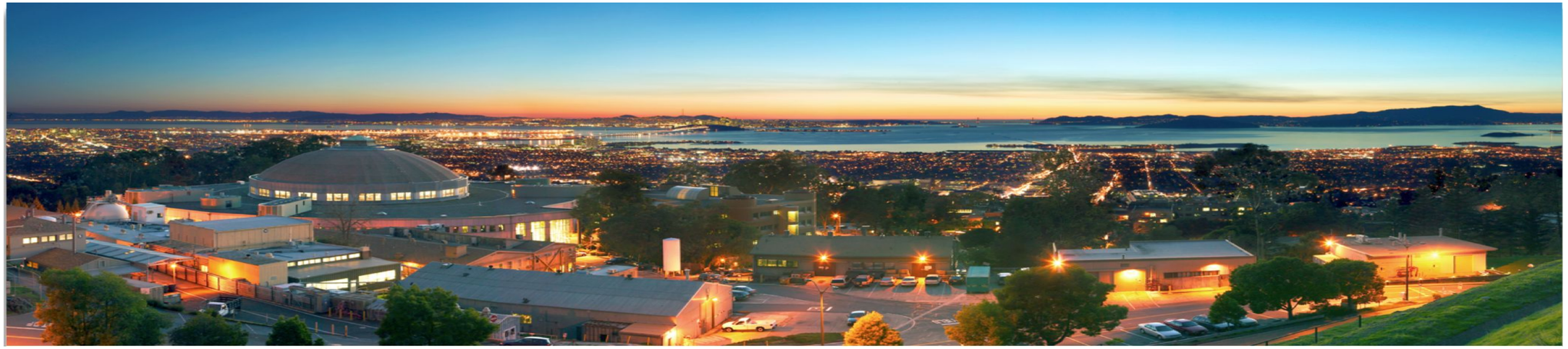


Supervisory Parameter Adjustment for Distribution Energy Storage (SPADES)

Year 1 Project Team Workshop

PI: Daniel Arnold

Dec. 2, 2020

U.S. DEPARTMENT OF ENERGY

UNIVERSITY OF CALIFORNIA

BERKELEY LAB
Lawrence Berkeley National Laboratory

Agenda

10:00 - 10:10: Project & Year 1 Overview (Dan Arnold - dbarnold@lbl.gov)

10:10 - 10:35: Storage and Control Module Architecture in PyCIGAR (Michael Sankur - msankur@lbl.gov &Sy-Toan Ngo - SyToanNgo@lbl.gov)

10:35 - 11:00: Grid Forming/following & Active Load Stability Simulation (Ciaran Roberts - cmroberts@lbl.gov)

11:00 - 11:25: Open Modeling Framework (OMF) Updates. Use Case Analysis, Network Reduction (David Pinney - dpinney@me.com & Lisa Slaughter - lisa.m.slaughter@gmail.com)

11:25 - 11:30: BREAK

11:30 - 11:55: Red Team Planning/Methodology (Bruno Leao - bruno.leao@siemens.com)

11:55 - 12:20: Log(V) 3LPF: A linearized solution to train reinforcement learning algorithms for unbalanced distribution systems (Ignacio Losada Carreno - ilosadac@asu.edu)

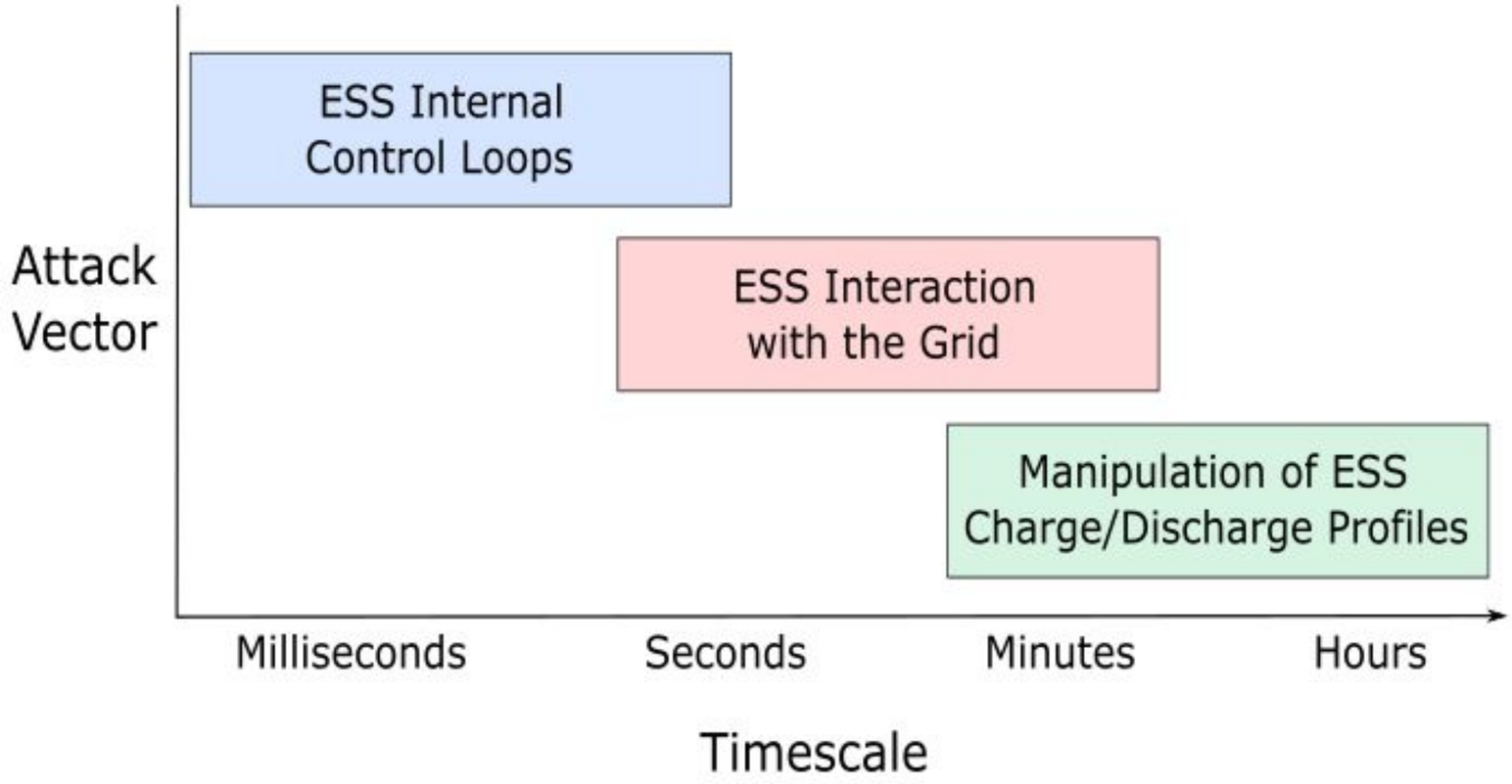
12:20 - 12:30: Concluding Remarks and Y2 Outlook (Dan Arnold - dbarnold@lbl.gov)

SPADES Project Overview

- Develop the methodology and tools allowing Electric Storage Systems (ESS), e.g battery storage, to automatically reconfigure themselves to counteract cyberattacks
- Defend against direct threats to the ESS control systems and indirect threats through the electric grid.
- Validate defensive algorithms in simulation and hardware experiments
- Integrate methodologies to mitigate cyber attacks against ESS into open source simulation tools

SPADES Threat Vectors

Focusing on 3 Threat Vectors (TV) for ESS that span multiple timescales



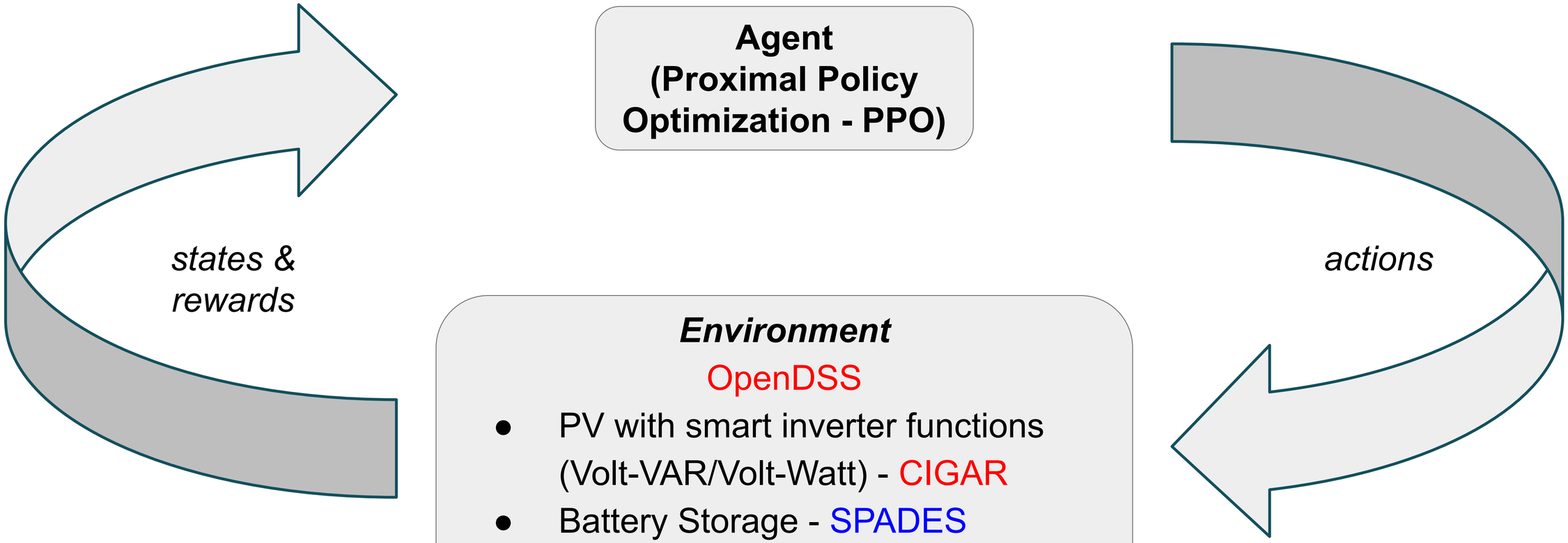
Threat Vectors

- **ESS Internal Control (<<1s):** An adversary updates a set of controller gains and/or user-defined set-points in order to cause the ESS to go internally unstable and damage itself, or trip offline to protect itself.
- **ESS/Grid Interaction (secs - mins):** Ad adversary gains controllability of a subset of devices on the network and conducts an attack to disrupt grid operations (e.g. create large voltage imbalances).
- **Charging/Discharging Control (mins - hours):** An adversary seeks to manipulate an ESS's charging and/or discharging schedule to impact ESS providing grid services (e.g maliciously discharging the ESS in an islanded microgrid during PV generation hours so there is insufficient available power during non-generation hours

Remediation

- **ESS Internal Control (<<1s):** Develop a supervisory controller to reset control gains to maintain stable state of operation. Supervisory control system validated via transient simulation capabilities in Julia
- **ESS/Grid Interaction (secs - mins):** Extend CIGAR reinforcement learning control framework to include storage dynamics and ESS grid services (e.g. peak shaving, smoothing etc.)
- **Charging/Discharging Control (mins - hours):** Extend CIGAR RL framework, with the inclusion of SoC temporal dynamics and service delivery options, to allow an ESS to locally implement a cyber-resilient charging/discharging policy.

Reinforcement Learning Training Loop



SPADES Y1 Accomplishments

- Task 1 - Feedback Control Modeling of ESS/Electric Grid Interaction (COMPLETE on 12/31/2020)
  - Developed models of ESS power electronic control systems and associated simulations
  - Developed models of storage SOC dynamics and integrated into CIGAR software framework
  - Investigated use of linearized power flow model to improve reinf. learning training time
  - Cataloged storage use cases applicable to NRECA co-ops
- Task 2 - Supervisory Control System Development
  - Developed adaptive control approach to use ESS to mitigate certain attacks on the electric grid
- Task 3 - Hardware-In-the-Loop Experiment and Red Team Attack
  - Red team scoping activity underway
- Task 4 - Open Modeling Framework (OMF) Integration
  - Extension of CIGAR OMF capabilities to include storage
  - OpenDSS network reduction

Team Presentations