Exhibit A - Statement of Work

This Research Statement of Work is made and entered into effective the 15th day of April, 2018 by Eversource Energy Service Company, for itself and as agent for its affiliates, having principal offices at 107 Selden Street, Berlin, CT 06037 ("Company") and UNIVERSITY OF CONNECTICUT ("University") pursuant to the terms of the SECOND AMENDED AND RESTATED SPONSOR RESEARCH AND SERVICES AGREEMENT between Company and University dated May 1st, 2015 (the "Sponsor Research Agreement").

Both Parties agree to participate in Research to be conducted in accordance with the terms and conditions of the Sponsor Research Agreement and this Research Statement of Work, provided however, that in the event of a conflict between the terms and conditions of the Sponsor Research Agreement and this Research Statement of Work, the terms of the Sponsor Research Agreement shall be controlling.

1. **Title of Research/Project:**
   Modeling, Analysis and Anomaly Detection for Cyber Secure Eversource Power Distribution Networks: Phase I
2. **Research/Project Description:**
   - **A. Problem Statement**
   - **B. Proposal Objectives**
   - **C. Methodology**
   - **D. Data requirements**
   - **E. Project Deliverables**
   - **F. Project Timetable and Milestones: 04/15/2018 – 05/31/2019**

University of Connecticut

By PI: Peng Zhang

Printed Name: Peng Zhang

Title: Professor

Date: 04/12/2018

The Connecticut Light and Power Company doing business as Eversource Energy

By:

Printed Name: SAMUEL WOOLARD

Title: Director Distribution Engineering

Date: 04-24-18

By Sponsored Program Services:

Printed Name: Laura Kozma

Title: Director

Date: 4/13/18

problems of identifying attacks, intercepting threats in realistic settings of the Eversource Energy networks.

The main tasks include modeling the cyber power distribution system for Eversource Energy, detecting the threats of power-bot attacks on power distribution systems in representative scenarios, designing Power-Wall, an effective defense mechanism protecting the grid from the end-devices and preventing attacks on power grid operations and data. It offers unique and powerful cyber tools for utility companies that unify cyber-physical grid dynamics information, multi-level cyber-protection mechanisms with cyber-physical-systems approaches.

The proposed modeling, analysis, detection and mitigation methods will be prototyped and thoroughly validated on the Eversource Energy grids implemented on UConn's cyber-physical power grid testbed [1] developed through several major National Science Foundation (NSF) and Department of Energy (DOE) projects.

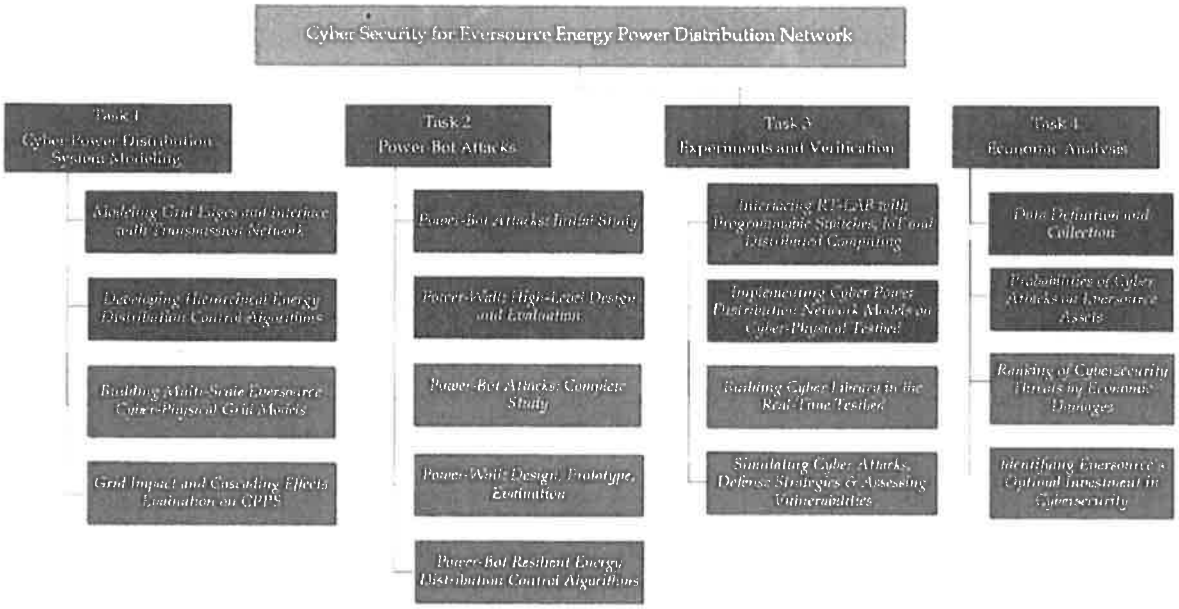
Cyber Security for Eversource Energy Power Distribution Network
Task 1
Cyber Power Distribution System Modeling
Modeling Grid Edges and Interface with Transmission Network
Developing Hierarchical Energy Distribution Control Algorithms
Building Multi-Scale Eversource Cyber-Physical Grid Models
Grid Impact and Cascading Effects Evaluation on CPPS
Task 2
Power-Bot Attacks
Power-Bot Attacks: Initial Study
Power-Wall: High-Level Design and Evaluation
Power-Bot Attacks: Complete Study
Power-Wall: Design, Prototype, Evaluation
Power-Bot Resilient Energy Distribution Control Algorithms
Task 3
Experiments and Verification
Interfacing RT-LAB with Programmable Switches, IoT and Distributed Computing
Implementing Cyber Power Distribution Network Models on Cyber-Physical Testbed
Building Cyber Library in the Real-Time Testbed
Simulating Cyber Attacks, Defense Strategies & Assessing Vulnerabilities
Task 4
Economic Analysis
Data Definition and Collection
Probabilities of Cyber Attacks on Eversource Assets
Ranking of Cybersecurity Threats by Economic Damages
Identifying Eversource's Optimal Investment in Cybersecurity

Fig. 1: Structure of the project (Phase I subtasks highlighted in blue; Phase II subtasks in green)

The PIs will disseminate their security solutions through Eversource Energy Center to major power utilities, power technology vendors, EPRI and national laboratories. The expectation of the team is to obtain 1-2 major federal grants by the 2nd year of this project by leveraging the outcomes of this pilot project.

This project will be conducted in two phases: Phase I (04/15/2018-5/31/2018) and Phase II (06/01/2019-5/31/2020).

B. Project Objectives

Our proposed research and development efforts in Phase I will be described in the following four tasks. As a major effort of this project, the research team will closely work Eversource to devices, in particular, by exploiting cyber-attacks. We refer to such devices, connected to the power network (as consumers or providers of energy), yet controlled by an attacker, as power-bots, and to the collection of all of these devices controlled by the attacker as a power-botnet.

There are different scenarios in which power-bots and power-bot networks such devices may become a threat to the power grid. We consider the following scenarios:

- Normal Operation of Large Distribution Grid. Under normal operational conditions, large distribution network can be a target for malicious, well-equipped and well-motivated adversaries, which control a power-botnet. Potential attacks may include: faking the DER/microgrid connection to or disconnection from the grid; compromising critical loads; changing the settings of protection relays causing the relays to trip erroneously or to get stuck; jamming communication channels; triggering arbitrary reclosing or opening of circuit breakers; etc. These attacks can jeopardize the normal operation of the power distribution networks and can be highly dangerous.
- Grid restoration. When severe damages or a total blackout occurs, distribution grid restoration is the most critical process to recover power supply, including energizing distribution feeders, cranking DERs and microgrids and re-synchronizing them into distribution grid, and load recovery. Cyber-attacks, esp. exploiting power-bots and power-botnets, may significantly compromise this process, preventing power restoration, or leading to a painfully long process of customer power restoration and sustained outages.
- Islanding and micro-grids. A major challenge caused by cyber-attacks is the unintentional islanding of a feeder, which can create safety hazards for utility customers and field crews. Attackers can mimic normal grid conditions through deception attacks, which makes DER units continue to energize power lines from customers' homes or businesses. Alternatively, as intentional, controlled microgrids are designed to provide continuous operations when the 'large' grid fails, power-bot attacks may disrupt the micro-grid or its re-connection to the 'large' grid.

In this task, we will study the threat of Power-Bots and develop an innovative defense, the Power-Wall. The Power-Wall is a device connecting a consumer (residence, company, organization) or a DER to the grid, possibly within a microgrid. The basic function of the Power-Wall is to protect the grid (and/or microgrid) from attacks or other disruptions from the consumer/DER, including attacks or disruptions which are synchronized among multiple consumers/DERs.

Power-Walls are reminiscent of the Firewalls usually used in the connection between a home/office network and the Internet, however, Power-walls prevent attacks on the actual power consumption/production and not (only) on data; note also that the basic function of power-walls is to protect the grid from the end-devices rather than protect the home/office network from attackers from the Internet.

We identify the following sub-tasks in Phase I of the project:

- Task 2.1. Power-Bot Attacks: initial study. In this task we study power-bots attacks, focusing on attacks designed to disrupt operations in microgrids and/or parts of grid. Our

While the need for cybersecurity in contemporary electric utilities is clear, the expected benefits of cybersecurity investment are more difficult to quantify. This task focuses on the challenge of measuring the benefits of cybersecurity investment in terms of identifying probabilities and expected damages of specific types of attacks. Specifically, this task will help identify the types of attacks and devices that would cause the most economic damage in order to direct cybersecurity investment to the most impactful areas. The critical questions this task seeks to answer are:

- What are the probabilities of specific types of cyberattack on specific Eversource assets?
- What is the expected economic value of damages sustained by Eversource and stakeholders conditional on a specific type of attack on a specific asset?
- What is the ranking of cybersecurity priorities for Eversource based on expected economic damage from each type of attack?
- What is the cumulative capital budget necessary to prevent a target percentage of economic damage from the top N% of attacks ranked by expected economic damage?

These four questions will be addressed through four objectives:

Objective 1: Data definition and collection. We will also need to estimate the probability and economic damage from incurring a preventable cyberattack. Cyberattacks are rare events, so their impact will be hard to measure ex-ante. We will need significant input from Eversource to determine their value, vulnerability, and costs they would face as a cyberattack target. We will also leverage our contacts to generate a list of potential types of cyberattacks and their targets.

Objective 2: Use testbed simulation to generate average probabilities of different types of cyberattack on different types of Eversource assets, as well as expected economic damage to the firm and customers from these attacks. Quantifiable damage will include Eversource hardware losses, customer costs from power outages, costs of disruption or interference with Eversource operations, and Eversource reputational costs from incurring a successful cyberattack.

Objective 3: Create a ranking of potential cybersecurity threats by expected economic damage incurred. This will enable the computation of a cybersecurity budget based on some cumulative fraction of total potential economic damage from cyber threats to Eversource and stakeholders.

Objective 4: Identify Eversource's optimal investment in cybersecurity using the Gordon-Loeb model. The Gordon-Loeb model is the first economic model to be developed for calculating the optimal investment in cybersecurity in particular. Depending on the assessed vulnerability of the system, as well as the expected damage from a successful cyberattack, this model provides recommendations for optimal spending as a fraction of the firm's budget.

In Phase I of this project, we will focus on Objectives 1 and 2 while we will achieve Objectives 3 and 4 in Phase II.

D. Data Requirements

Eversource Energy Engineering department will provide models and data for selective feeders and sub- stations and metering data for load and distributed generation. Eversource IT

- Complete initial evaluation (simulation) of power-bot attacks, and their impact on Eversource grid (Herzberg, Zhang and Miao).
- Complete high-level design and initial evaluation of Power-Wall defense (Herzberg, Zhang and Miao).
- Deliver first-year report (slide show and/or document) and detailed plan for second year (Herzberg, Zhang and Miao).

Task 3: Experiments and Validation (Zhang, Miao, Herzberg, and Borochin)

Year 1, Quarter 1

- Acquire detailed OT, IT and grid feeder data from Eversource Energy.

Year 1, Quarter 2

- Interface RT-LAB simulator interfaced with 8 HP and SEL OpenFlow switches that can emulate complex programmable communication networks.
- Test and debug the test backbone distribution grid on the RT-LAB simulator.

Year 1, Quarters 3&4

- Test and debug the cyber-physical distribution grid models on the RT-LAB simulator.
- Assess the effect of power bot attacks on feeders, microgrids and DERs with virtual/SDN networks and run what-if scenarios about critical infrastructure under cyber-attack.
- Write fist-year report, prepare for publications.

Task 4: Economic Analysis of Cybersecurity Threats and Solutions (Borochin, Zhang, Herzberg, and Miao)

Year 1, Quarter 1

- Data collection and meetings with Eversource IT staff.
- Identify primary assets and attack goals.

Year 1, Quarter 2

- Data collection and meetings with Eversource IT staff (continued).
- Identify primary assets and attack goals.

Year 1, Quarters 3&4

- Identify primary assets and attack goals in the established risk management context.
- Preliminary estimation of optimal IT investment using the Gordon-Loeb model based on collected data.
- Preliminary estimation of expected costs of cybersecurity attacks using the real options model based on collected data.
- Collaboration with testbed group to model probability distribution of cyberattacks for real option analysis.
- Deliver first-year report and detailed plan for second year.

F. Acceptance Criteria:

Fei Miao is an Assistant Professor that recently joined UConn. Dr. Miao has pioneered attack detection and secure control algorithms of cyber-physical systems based on physical dynamic models, control theory and optimization. Dr. Miao has been doing research on coding schemes for stealthy data injection attacks detection, and hybrid dynamic stochastic game schemes for resilient control strategies, as a Ph.D student team member of the DARPA HACMS project.

Paul Borochin is an Assistant Professor of Finance at UConn. He got his Ph.D. in Finance from the Fuqua School at Duke University and his B.S. in Finance and Statistics from the Wharton School at the University of Pennsylvania. Dr. Borochin's research areas are institutional ownership and applications of asset pricing theory to extract information about corporate events and policies, with sub-specializations in corporate governance, information asymmetry, and M&A. His recent interests also include evaluating economic impact of engineering solutions for power grid resilience.

Team's Existing Equipment and Facilities

Our team is equipped with a cyber-physical distribution testbed with the following features:

- Flexible and distributed testbed architecture. Our testbed is built following key principles including modularity, abstraction, federation, remote open-access capability, and reconfigurability. It includes the distribution infrastructure layer, communication/network layer and application layer.
- Real-time simulator for small or medium scale grid studies. Within the infrastructure layer, real life distribution feeder or microgrid performance can be modeled in various time-scales with high fidelity (In Phase II, the testbed will be equipped with ePHASORsim which will allow modeling CT grid in real-time with DERs dynamics, faults and disturbances). We will start developing the automated testing capability, which will make it particularly suitable for massive scenario checks to test thousands of attack scenarios.
- Supporting industrial communication protocols. The testbed will integrate the data concentrators, Human Machine Interfaces, SDN switches, GPS satellite clocks and six protective relays/PMUs developed or obtained from our DOE and NSF projects.

I. Budget

The budget for Phase I will be $150,000 with the breakdown of costs per topics summarized below for projects dates April 15, 2018 through May 31, 2019.

	Date (mm/yyyy)	Task	Budget
Phase I	04/2018	Task 1, 2, 3	$80,000
	08/2018	Tasks 1, 2, 3, 4	$70,000