2020

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS

# CEDS PEER REVIEW

*Virtual Edition*

U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

# TUESDAY – OCTOBER 6, 2020

| | | | |
|---|---|---|---|
| 10:00 – 10:30 | **REGISTRATION CHECK-IN AND VIRTUAL SETUP** | | |
| 10:30 – 10:45 | **INSTRUCTIONS – WALTER YAMBEN** | | |
| 10:45 – 11:00 | **KEYNOTE SPEAKER** | | |
| 11:00 – 11:30 | General Electric (GE) Company | Time-Sensitive Quantum Key Distribution | **Quantum Information Science (QIS)** |
| 11:30 – 12:00 | Oak Ridge National Laboratory (ORNL) | ScalablE Quantum Cybersecurity for Energy Storage Systems (SEQCESS) | |
| 12:00 – 12:30 | Brookhaven National Laboratory (BNL) | A Prototype for Ultimate Secure Transmission and Analysis of Smart Grid Data on the Wire | |
| 12:30 – 01:00 | **LUNCH BREAK** | | |
| 01:00 – 01:30 | Pacific Northwest National Laboratory (PNNL) | Verification and Validation Assuring Reliability and Security (VARS) | **Verification & Validation** |
| 01:30 – 02:00 | Oak Ridge National Laboratory (ORNL) | A Cyber-Physical Security Assurance Framework Based on a Semi-Supervised Vetting (CYVET) | |
| 02:00 – 02:15 | **BREAK** | | |
| 02:15 – 02:45 | Sandia National Laboratories (SNL) | Energy Storage Security (ESSec) using Microservices | **Energy Storage** |
| 02:45 – 03:15 | Lawrence Berkeley National Laboratory (LBNL) | Supervisory Parameter Adjustment for Distribution Energy Storage (SPADES) | |
| 03:15 – 03:45 | ABB, Inc. | Security Enhancements for Distributed Energy Resource Systems in Standardized Institute of Electrical and Electronic Engineers 1547 Environments | **Advanced Communications** |
| 03:45 – 04:15 | ABB, Inc. | Cyber Resilient Flexible Alternating Current Transmission Systems | **Cybersecurity Innovation** |
| 04:15 – 04:30 | **BREAK** | | |
| 04:30 – 05:00 | Schweitzer Engineering Laboratories (SEL), Inc. | Ambassador | |
| 05:00 – 05:30 | Lawrence Livermore National Laboratory (LLNL) | Cyber Interconnection Analysis for High Penetration of DER | |

# WEDNESDAY – OCTOBER 7, 2020

| | | | |
|---|---|---|---|
| 10:00 – 10:45 | **REGISTRATION CHECK-IN AND VIRTUAL SETUP** | | |
| 10:45 – 11:15 | Texas A&M Engineering Experiment Station | Deep Cyber-Physical Situational Awareness for Energy Systems: A Secure Foundation for Next-Generation Energy Management | **Artificial Intelligence (AI)** |
| 11:15 – 11:30 | **KEYNOTE SPEAKER** | | |
| 11:30 – 12:00 | General Electric (GE) Company | Cyber-Physical Protection for Natural Gas Compression | |
| 12:00 – 12:30 | General Electric (GE) Company | Cyber-Physical Resilience for Wind Power Generation | |
| 12:30 – 01:00 | **LUNCH BREAK** | | **Artificial Intelligence (AI)** |
| 01:00 – 01:30 | Lawrence Berkeley National Laboratory (LBNL) | Cybersecurity via Inverter-Grid automatic Reconfiguration (CIGAR) | |
| 01:30 – 02:00 | Raytheon Technologies Research Center (formerly UTRC) | Watching Grid Infrastructure Stealthily Through Proxies | |
| 02:00 – 02:15 | **BREAK** | | |
| 02:15 – 02:45 | Dragos, Inc. | Neighborhood Keeper | |
| 02:45 – 03:15 | TDI Technologies, Inc. | Cognitive Sense and Decision Making Expert System for Adaptive Information Technology/Operational Technology Defense | **Threat Mitigation** |
| 03:15 – 04:15 | University of Arkansas | Center for Secure Evolvable Energy Delivery Systems (SEEDS) | |
| 04:15 – 04:30 | **BREAK** | | **Academic Consortium** |
| 04:30 – 05:30 | University of Illinois | Cyber Resilient Energy Delivery Consortium (CREDC) | |
| 05:30 – 06:00 | **PEER REVIEW CLOSE OUT - WRAP-UP AND COMMENTS/FEEDBACK** | | |

## ABB

### Security Enhancements for Distributed Energy Resource Systems in Standardized Institute of Electrical and Electronic Engineers 1547 Environments

The project objective is to develop cybersecure methods to implement the new Institute of Electrical and Electronics Engineers (IEEE) 1547-2018 use cases for the interconnection and interoperability of Area Electric Power Systems with Distributed Energy Resources (DER) facilities.

### Cyber Resilient Flexible Alternating Current Transmission Systems

ABB will develop methods and systems for defense-in-depth cybersecurity solutions of Flexible Alternating Current Transmission Systems (FACTS).

## BROOKHAVEN NATIONAL LABORATORY (BNL)

### A Prototype for Ultimate Secure Transmission and Analysis of Smart Grid Data on the Wire

The project plans to accomplish the following:

- Development of a prototype for an ultimately secure system in the context of energy delivery.
- Combine real or near-real time computations on streaming data in transit in the network together with quantum-protected key exchange.
- Provide hack-proof encryption to data flowing between different sources and destinations in the network while allowing intermediate smart network nodes to access the encrypted data
- Perform desired analysis on available real and simulated power grid data sets.

## DRAGOS

### Neighborhood Keeper

Dragos is researching, developing, and deploying an interconnected and trustworthy low-cost sensor network at the operational technology (OT) layer of utilities so that they gain access to threat detection while sharing the anonymized analytical outputs of that detection. This will enable an interconnection of rapidly adoptable technology across the sector that will facilitate a combined threat picture.

## GENERAL ELECTRIC (GE)

### Time-Sensitive Quantum Key Distribution

The project team will develop time-sensitive quantum key distribution, which leverages time-sensitive networking (TSN) and quantum key distribution (QKD) to increase the availability and integrity of cybersecurity for industrial control in the power industry.

### Cyber-Physical Resilience for Wind Power Generation

The project objective is to develop commercially viable and field-tested cyber protection technologies for wind power generation systems that are effective against control domain attacks at the physical layer of the system.

### Cyber-Physical Protection for Natural Gas Compression

The project team will develop a cyber-physical protection (CPP) system that minimizes damage to, and increases resiliency of, critical assets. CPP performs at the physical layer in conjunction with traditional information and operational technology cybersecurity. It uses advanced machine learning and control algorithms that are run via a new secure compute platform called EdgeOS.

# LAWRENCE BERKELEY NATIONAL LABORATORY (LBNL)

## Supervisory Parameter Adjustment for Distribution Energy Storage (SPADES)

The project will implement a supervisory controller that would reside on the energy storage system to prevent it from becoming unstable if setpoints are attacked. The project leverages LBNL efforts such as CIGAR and the GMLC 1.4.23 Threat Detection and Analytics project.

## Cybersecurity via Inverter-Grid automatic Reconfiguration (CIGAR)

The project team will develop supervisory control algorithms to counteract cyber-physical attacks that have compromised multiple independent systems in the electric grid. They will analyze the stability of different types of feedback control systems (e.g, distributed energy resources, and voltage regulation and protection systems) in the electric grid to determine what parameters an attacker would change if DER and utility voltage regulation and protection systems were compromised.

# LAWRENCE LIVERMORE NATIONAL LABORATORY (LLNL)

## Cyber Interconnection Analysis for High Penetration of DER

This project will develop and apply a cyber interconnection co-simulation tool, which will evaluate and analyze risk, and design mitigation strategies to address cyber-attacks on high penetration distributed energy resource (DER) systems. The tool will streamline analysis approaches for utilities and product vendors, to utilize best practices for cyber protection during interconnection, while not causing an increase in cost or time to interconnect.

# OAK RIDGE NATIONAL LABORATORY (ORNL)

### ScalablE Quantum Cybersecurity for Energy Storage Systems (SEQCESS)

The project objective is to research, develop, and transition nascent quantum physics-based technologies to improve the cybersecurity for supervisory control of distributed energy storage (DES) resources.

### A Cyber-Physical Security Assurance Framework Based on a Semi-Supervised Vetting (CYVET)

ORNL will develop a new specification framework in which cybersecurity requirements elements in standards presented in human-readable language can be expressed and transformed into machine-executable and verifiable formats.

# PACIFIC NORTHWEST NATIONAL LABORATORY (PNNL)

### Verification and Validation Assuring Reliability and Security (VARS)

PNNL will develop a publicly available V&V framework that will be realized in the form of an online tool that organizations can use to drive secure design and development of a product and make the V&V testing process formal and more consistent across different products, all while making room for tailoring testing to accommodate differences.

# RAYTHEON TECHNOLOGIES RESEARCH CENTER (formerly UTRC)

### Watching Grid Infrastructure Stealthily Through Proxies

Raytheon is developing tools and techniques for preventing and mitigating false data injection attacks (FDIAs) on Locational Marginal Pricing (LMP) nodes.

## SANDIA NATIONAL LABORATORIES (SNL)

### Energy Storage Security (ESSec) using Microservices

SNL is designing a secure and interoperable containerized suite of applications capable of operating an energy storage system. The team will include the ability to upgrade software in real-time, to quickly launch new applications as needed, to detect compromised or crashed applications using fault tolerant algorithms, and to manage a plethora of applications, such as Open Field Message Bus (OpenFMB) protocols adapters, within a variety of energy storage systems.

## SCHWEITZER ENGINEERING LABORATORIES (SEL)

### Ambassador

This project builds on the successful completion of the Watchdog and Software-Defined Networking (SDN) projects by researching, developing and demonstrating an engineered solution to manage the trust, data, and resources that are passed between software applications operating in the SDN eco-system.

## TDI TECHNOLOGIES

### Cognitive Sense and Decision Making Expert System for Adaptive Information Technology/Operational Technology Defense

TDi Technologies is developing a configuration management system for OT using a proven methodology used by information technology (IT), enabling importation of vulnerability alerts and enabling easy integration of system element information.

## TEXAS A&M ENGINEERING EXPERIMENT STATION

### Deep Cyber-Physical Situational Awareness for Energy Systems: A Secure Foundation for Next-Generation Energy Management

Texas A&M Engineering Experiment Stations will design a next generation secure energy management system that would enable stakeholders across energy industrial control domains to better prepare, mitigate, repair, and recover from cyber-related threats. The system will utilize a cyber-physical model, which is fed by data from field devices, vulnerability reports, firewall rules, alerts and cyber monitor logs.

## UNIVERSITY OF ARKANSAS

### Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS)

The project objective is to sponsor academic research and development of innovative cybersecurity technologies, tools and methodologies that will advance the energy sector's ability to survive cyber attacks and incidents while sustaining critical functions.

## UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

### Cyber Resilient Energy Delivery Consortium (CREDC)

The project objective is to sponsor academic research and development of innovative methodologies and technologies that will enable energy delivery systems (EDS) to continue to provide critical operations and deliver energy even while those systems are maliciously compromised through their supporting systems and communication infrastructure.

For more information please visit

energy.gov/ceser