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

Large-Scale Control Cybersecurity Testing Based on an Extended Testbed

SEEDS
CYBERSECURITY CENTER FOR
SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Developing a realistic testbed to simulate inter-substation communications during Alpha testing

The project team developed an extended testbed focusing on integrating virtual and physical assets along with virtual appliances, which are used to emulate Wide Area Networks (WANs) to simulate inter-substation communications. These virtual assets use existing physical assets, such as the OPAL-RT Real-Time simulator, along with various server resources. Virtual protection relays were developed using the real-time simulator along with virtual microgrid simulations. These relays were configured to communicate with physical assets using IEC 61850, DNP3, and Modbus-TCP protocols with analog voltage and current outputs. Virtual WAN interfaces were emulated using VMware Hypervisors and GNS3, which allows the virtualization of routers and switches, enabling the emulation of industrial networks. Additionally, multiple virtual servers were configured and connected to these virtual networks, serving functions such as supervisory control and data acquisition, security, and real-time monitoring. This extended testbed provided realistic inter-station level system integration testing capabilities.

KEY TAKEAWAYS

- Configures and integrates physical assets into a testbed
- Develops and integrates grid models and virtual protection relays to enable the evaluation of system-level impacts
- Delivers a realistic Alpha test environment with physical and virtual assets

OUTCOME

This project develops and delivers a realistic testbed for inter-substation communications, as they are related to the management and monitoring of the power grid, to facilitate the development and testing of cybersecurity-related mitigation strategies. The testbed has completed Alpha testing for many SEEDS-related projects and served as a remote laboratory for researchers. This extended testbed was the continuation of earlier work titled “Design and Development of the NCREPT-Based Security Testbed” and was primarily focused on adding additional communication and virtual assets.

PARTICIPANTS	ROLE
SEEDS CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS	This project is part of the Secure Evolvable Energy Delivery Systems (SEEDS) academic consortium. SEEDS researches and develops innovative cybersecurity technologies, tools, and methodologies to advance the energy sector’s ability to survive cyber incidents while sustaining critical functions.
UNIVERSITY OF ARKANSAS	Engages with fellow researchers to define a testbed with the capabilities needed to Alpha test potential solutions. Develops the testbed to meet given specifications and performs system-level testing to verify efficacy of partner research organizations’ solutions.

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Jia Di
Principal Investigator
University of Arkansas
479-575-5728
jdi@uark.edu

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

This is a subproject sponsored by the SEEDS academic consortium, led by the University of Arkansas.

SEEDS Period of Performance: October 2015 – March 2022

SEEDS Total Award Value: $15,309,114
DOE Share: $12,226,504
Cost Share: $3,082,610

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation’s energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: June 2021