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

Bulk Electric Systems Supply Chain Cyber Risk Management

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

A permissioned blockchain for energy sector procurement and risk mitigation

Many critical components of bulk energy systems are manufactured by various overseas suppliers and are distributed and integrated into energy delivery systems (EDS) by a multitude of vendors. Each step of this cyber supply chain introduces unique threats and vulnerabilities, and expands the potential attack surfaces for EDS. This project develops a permissioned blockchain platform to provide early detection and reporting of faults in EDS supply chain and procurement. The approach incorporates cyber risk management into a blockchain-based procurement process. The customer outlines component performance and security requirements on a blockchain ledger through which the participating vendor identifies the appropriate hardware and/or software suppliers. The details are then reported back to the ledger. This process allows the customers to improve auditability, attribution, and provenance of their critical assets. The system also integrates vulnerability databases that report to the stakeholders any potential vulnerability risks in a component. The supplier will provide remediation plans to be validated via the permissioned blockchain.

KEY TAKEAWAYS

- Applies permissioned blockchain services to mitigate cyber risk in energy system procurement and management procedures
- Validates the authenticity of customer/supplier identities, system components, and risk remediation details
- Improves auditability, accountability, and attribution in cyber risk management

OUTCOME

The developed tool enhances trust in system components and in cyber-risk mitigation strategies for reliable and resilient EDS infrastructures. Committing procurement details to the blockchain ledger guarantees that all faults and/or security risks introduced into EDS networks are attributable. This minimizes malicious intervention in the bulk energy cyber supply chain.

PARTICIPANTS	ROLE
CREDC Cyber Resilient Energy Delivery Consortium	The CREDC performs multidisciplinary research and development that focuses on the cybersecurity of energy delivery systems. The central project goal is to create an ecosystem where research results lead directly to the development of applications and methodologies, which are then validated in realistic contexts.
Old Dominion University	Leads research, development, and testing
RF ReliabilityFirst	Collaborates with the academic team on tool testing, evaluation, and deployment

CONTACT INFORMATION

Initial Leads:

Sachin Shetty
Site Lead, Associate Professor
Old Dominion University
757-686-6233
sshetty@odu.edu

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 CREDC academic consortium, led by the University of Illinois.

CREDC Period of Performance: October 2015 – May 2022

CREDC Total Award Value: $28,099,258
DOE Share: $22,476,290
Cost Share: $5,622,968

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