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

Creating an Energy Delivery System Cyber Safety Analysis Discipline

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Applying lessons learned from prior incidents to a more holistic approach to energy delivery system security

Energy delivery system (EDS) organizations strive diligently to protect the key components of their infrastructures, but often serious hazards occur at interfaces between the physical, cyber, and human systems and subsystems, requiring a more holistic approach. The cybersafety analysis discipline (CAD) introduces a new way of thinking about the complex and dynamic EDS environment. CAD is based on an adaption of the System-Theoretic Accident Model and Processes (STAMP), originally developed for accident or incident analysis for use in situations such as the Challenger Space Shuttle disaster. STAMP organizes the overall system as a hierarchy of control loop structures, where constraints at higher levels control behavior at lower levels. CAD applies STAMP's holistic system view methodology to address and eliminate serious cyber hazards in EDS and implements effective countermeasures during design and/or operation to prevent losses.

KEY TAKEAWAYS

- Evaluates energy delivery system infrastructures as complex hierarchies of interconnected components instead of individually managed elements
- Identifies and eliminates potential security risks at system-subsystem interfaces
- Equips energy delivery system operators with a holistic view of system states to better implement security controls and countermeasures

OUTCOME

The CAD approach identifies and mitigates critical security flaws across the interconnections of EDS infrastructure, ranging from access points into secure systems to entry pathways via unsecured auxiliary components, such as security cameras in EDS control facilities. This hierarchical approach gives EDS operators a more holistic understanding of their security posture and minimizes the risk of human error in system security and operation.

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.
Massachusetts Institute of Technology	Lead institution; engages with MIT cogeneration facility as data source and for concept demonstration
ExxonMobil	Engages oil and gas stakeholders
New York Power Authority	Engages utility stakeholders
Schneider Electric	Engages industry stakeholders

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Stuart Madnick
Site Lead, Professor
Massachusetts Institute of Technology
617-253-6671
smadnick@mit.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 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