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

Reliability and Cyber-Physical Threat Model Generation from a Standards Influenced Ontology

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Cutting edge complex modeling tools to advance cyber-physical system resilience

The research team is developing a theoretically sound methodology and tools that enable energy delivery system (EDS) stakeholders to model cyber adversaries, identify likely attack paths, and select countermeasures to thwart attackers. This project is based on the ADversary View Security Evaluation (ADVISE) modeling framework within the Möbius tool, a platform that models the behavior of complex systems. The team will extend ADVISE to comprehend the underlying physical infrastructure of the EDS, enabling the creation of inter-connected models that more accurately represent and simulate unique systems. This tool will generate comprehensive, useful, random models to explore the reliability and security of EDS and to estimate system impact through cyber-physical attack simulations.

KEY TAKEAWAYS

- Advances complex modeling of energy delivery systems for comprehensive situational awareness
- Generates useful stochastic models to explore energy delivery system reliability and security
- Simulates cyberattacks within complex attack graph models to enhance understanding of threat vectors and intermediate system component vulnerabilities

OUTCOME

This project delivers new concepts for generating complex EDS models that provide a rich, flexible way for examining the reliability of systems and their constituent components. EDS operators will get a highly accurate and comprehensive view of the possible attack paths and vulnerabilities within complex cyber-physical systems, advancing security and system reliability.

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.
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN	Leads research, development, and testing
ABB	Engages industrial stakeholders
DUKE ENERGY®	Engages utility stakeholders

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Ken Keefe
Senior Software Engineer
University of Illinois
217-244-3203
kjkeefe@illinois.edu

Alfonso Valdes
Principal Research Scientist,
Information Trust Institute
University of Illinois
217-244-5147
avaldes@illinois.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